

全国计算机技术与软件专业技术
资格（水平）考试用书

网络工程师考试 考前冲刺与考点分析

希赛教育软考学院 主编

考点脉络

总结和归纳
考试必备的知识点

+

考点精讲

“画龙点睛” 考点脉络
部分中列出的重点

+

考前冲刺

提供了整个学科
体系的强化练习，
使读者做到举一反三

打通软考任督二脉



电子工业出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
<http://www.phei.com.cn>

全国计算机技术与软件专业技术资格（水平）考试用书

网络工程师考试考前冲刺 与考点分析

希赛教育软考学院 主编

電子工業出版社·

Publishing House of Electronics Industry

北京·BEIJING

内 容 简 介

本书由希赛教育软考学院主编，作为计算机技术与软件专业技术资格（水平）考试中的网络工程师级别的考试辅导指定教材。在参考和分析历年试题的基础上，根据最新的考试大纲进行内容的组织。全书每章节按照考点脉络、考点精讲、一点一练、考前冲刺、习题解析的体系进行讲解。

准备参加考试的人员可通过阅读本书掌握考试大纲规定的核心知识，把握考试重点和难点，熟悉考试方法、试题形式、试题的深度和广度，以及解答问题的方法和技巧等。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目（CIP）数据

网络工程师考试考前冲刺与考点分析 / 希赛教育软考学院主编. —北京：电子工业出版社，2013.7
全国计算机技术与软件专业技术资格（水平）考试用书
ISBN 978-7-121-20499-9

I. ①网… II. ①希… III. ①计算机网络—工程技术人员—资格考试—自学参考资料 IV. ①TP393

中国版本图书馆 CIP 数据核字（2013）第 109274 号

责任编辑：孙学瑛

印 刷：北京中新伟业印刷有限公司

装 订：三河市皇庄路通装订厂

出版发行：电子工业出版社

北京市海淀区万寿路 173 信箱 邮编：100036

开 本：787×1092 1/16 印张：27 字数：741.3 千字

印 次：2013 年 7 月第 1 次印刷

定 价：59.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zltz@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前 言

全国计算机技术与软件专业技术资格（水平）考试（俗称“软考”）由人事部、工业和信息化部主办，面向社会，用于考查计算机专业人员的水平与能力。考试客观、公正，得到了社会的广泛认可，并实现了中、日、韩三国互认。

本书紧扣考试大纲，基于每章节知识点分布统计分析的结果，科学地编写强化练习题，结构科学、重点突出、针对性强。

内容超值，针对性强

本书每章的内容分为考点脉络、考点精讲、一点一练、考前冲刺、习题解析五部分。

第一部分为考点脉络。对考试大纲中所规定的重要考试内容和考试必备的知识点进行总结 and 归纳，为读者指引学习方向。

第二部分为考点精讲。对考点脉络部分中列出的重要知识点进行“画龙点睛”，对章节中知识点解析的深浅程度根据该知识点在历年试题中的统计分析结果而定。通过学习本部分内容，考生可以对考试的知识点分布、考试重点有一个整体上的认识和把握。

第三部分为一点一练。针对每个知识点，给出了多道试题，根据考点精讲部分的知识点统计、分析的结果而命题。这些试题与考试真题具有很大的相似性，用来检查考生学习的效果。

第四部分为考前冲刺。读者在掌握了每个细节知识点之后，本部分为读者提供了整个学科体系的强化练习，使读者做到举一反三，从根本上掌握本章的考点。

第五部分为习题解析。习题解析部分是考前冲刺部分的补充，为考前冲刺的所有习题进行了较详细的分析，并给出了解答。考生需要掌握每个练习题及其解答，这一部分可以帮助考生温习和巩固前面所学的知识，这种辅导方式保证内容全面，突出重点，为考生打造一条通向考试终点的捷径。

作者权威，阵容强大

希赛教育（www.educity.cn）专业从事人才培养、教育产品开发、教育图书出版，在职业教育方面具有极高的权威性。特别是在在线教育方面，稳居国内首位，希赛教育的远程教育模式得到了国家教育部门的认可和推广。

希赛教育软考学院是全国计算机技术与软件专业技术资格（水平）考试的顶级培训机构，拥有近 20 名资深软考辅导专家，负责了高级资格的考试大纲制订工作，以及软考辅导教材的编写工作，共组织编写和出版了 80 多本软考教材，内容涵盖了初级、中级和高级的各个专业，包括教程系列、辅导系列、考点分析系列、冲刺系列、串讲系列、试题精解系列、疑难解答系列、全程指导系列、案例分析系列、指定参考用书系列、一本通等 11 个系列的书籍。希赛教育软考学院的专家录制了软考培训视频教程、串讲视频教程、试题讲解视频教程、专题讲解视频教程等 4 个系列的软考视频，希赛教育软考学院的软考教材、软考视频、软考辅导为考生助考、提高通过率做出了不可磨灭的贡献，在软考领域有口皆碑。特别是在高级

资格领域，无论是考试教材，还是在线辅导和面授，希赛教育软考学院都独占鳌头。

本书由希赛教育软考学院组织编写，参加编写工作的人员有张友生、王勇、李雄、胡钊源、桂阳、何玉云、王玉罡、胡光超、左水林、刘中胜、刘洋波。

在线测试，心中有数

上学吧（www.shangxueba.com）在线测试平台为考生准备了在线测试，其中有数十套全真模拟试题和考前密卷，考生可选择任何一套进行测试。测试完毕，系统自动判卷，立即给出分数。

对于考生做错的地方，系统会自动记忆，待考生第二次参加测试时，可选择“试题复习”。这样，系统就会自动把考生原来做错的试题显示出来，供考生重新测试，以加强记忆。

如此，读者可利用上学吧在线测试平台的在线测试系统检查自己的实际水平，加强考前训练，做到心中有数，考试不慌。

诸多帮助，诚挚致谢

在本书出版之际，要特别感谢全国软考办的命题专家们，为了使本书的习题与考试真题逼近，编者在写作中参考了部分考试原题。在本书的编写过程中，还参考了许多相关的文献和书籍，编者在此对这些参考文献的作者表示感谢。

感谢电子工业出版社孙学瑛老师，她在本书的策划、选题的申报、写作大纲的确定，以及编辑、出版等方面，付出了辛勤的劳动和智慧，给予了我们很多的支持和帮助。

感谢参加希赛教育软考学院辅导和培训的学员，正是他们的想法汇成了本书的原动力，他们的意见使本书更加贴近读者。

由于编者水平有限，且本书涉及的内容很广，书中难免存在错漏和不妥之处，编者诚恳地期望各位专家和读者不吝指正和帮助，对此，我们将十分感激。

互动讨论，专家答疑

希赛教育软考学院是中国最大的软考在线教育网站，该网站论坛是国内人气最旺的软考社区，在这里，读者可以和数十万考生进行在线交流，讨论有关学习和考试的问题。希赛教育软考学院拥有强大的师资队伍，为读者提供全程的答疑服务，在线回答读者的提问。

有关本书的意见反馈和咨询，读者可在希赛教育软考学院论坛“软考教材”版块中的“希赛教育软考学院”栏目上与作者进行交流。

希赛教育软考学院
2013年5月

目 录

第 1 章 计算机硬件基础	1	3.2 系统开发基础	63
1.1 考点脉络	1	3.2.1 考点精讲	63
1.2 计算机组成	1	3.2.2 一点一练	79
1.2.1 考点精讲	1	3.2.3 解析与答案	81
1.2.2 一点一练	7	3.3 项目管理	82
1.2.3 解析与答案	8	3.3.1 考点精讲	82
1.3 数据运算	11	3.3.2 一点一练	88
1.3.1 考点精讲	11	3.3.3 解析与答案	90
1.3.2 一点一练	13	3.4 考前冲刺	92
1.3.3 解析与答案	14	3.5 习题解析	94
1.4 存储体系与寻址方式	17	第 4 章 知识产权与标准化	98
1.4.1 考点精讲	17	4.1 考点脉络	98
1.4.2 一点一练	21	4.2 知识产权	98
1.4.3 解析与答案	22	4.2.1 考点精讲	98
1.5 中断、流水线以及性能评估	25	4.2.2 一点一练	105
1.5.1 考点精讲	25	4.2.3 解析与答案	106
1.5.2 一点一练	28	4.3 标准化法	107
1.5.3 解析与答案	30	4.3.1 考点精讲	107
1.6 考前冲刺	33	4.3.2 一点一练	109
1.7 习题解析	37	4.3.3 解析与答案	110
第 2 章 操作系统	44	4.4 考前冲刺	111
2.1 考点脉络	44	4.5 习题解析	112
2.2 存储和进程管理	44	第 5 章 网络体系结构	115
2.2.1 考点精讲	44	5.1 考点脉络	115
2.2.2 一点一练	52	5.2 参考模型	115
2.2.3 解析与答案	53	5.2.1 考点精讲	115
2.3 文件管理	54	5.2.2 一点一练	118
2.3.1 考点精讲	54	5.2.3 解析与答案	118
2.3.2 一点一练	55	5.3 各种协议	120
2.3.3 解析与答案	57	5.3.1 考点精讲	120
2.4 考前冲刺	58	5.3.2 一点一练	127
2.5 习题解析	60	5.3.3 解析与答案	128
第 3 章 计算机系统开发基础	63	5.4 考前冲刺	132
3.1 考点脉络	63	5.5 习题解析	133

第 6 章 数据通信基础	138
6.1 考点脉络	138
6.2 数据通信基础技术	138
6.2.1 考点精讲	138
6.2.2 一点一练	142
6.2.3 解析与答案	144
6.3 传输交换与差错控制技术	147
6.3.1 考点精讲	147
6.3.2 一点一练	151
6.3.3 解析与答案	152
6.4 考前冲刺	153
6.5 习题解析	156
第 7 章 局域网技术	161
7.1 考点脉络	161
7.2 介质、网络设备、 综合布线系统	161
7.2.1 考点精讲	161
7.2.2 一点一练	168
7.2.3 解析与答案	170
7.3 以太网技术和无线局域网	172
7.3.1 考点精讲	172
7.3.2 一点一练	179
7.3.3 解析与答案	180
7.4 虚拟局域网	183
7.4.1 考点精讲	183
7.4.2 一点一练	186
7.4.3 解析与答案	188
7.5 考前冲刺	191
7.6 习题解析	195
第 8 章 广域网和接入网技术	206
8.1 考点脉络	206
8.2 广域网	206
8.2.1 考点精讲	206
8.2.2 一点一练	211
8.2.3 解析与答案	212
8.3 接入网	213
8.3.1 考点精讲	213
8.3.2 一点一练	216
8.3.3 解析与答案	216
8.4 考前冲刺	219
8.5 习题解析	220

第 9 章 因特网与网络互联技术	224
9.1 考点脉络	224
9.2 IP 地址	224
9.2.1 考点精讲	224
9.2.2 一点一练	232
9.2.3 解析与答案	233
9.3 路由技术及路由协议	235
9.3.1 考点精讲	235
9.3.2 一点一练	244
9.3.3 解析与答案	246
9.4 NAT、ACL 及路由器常规配置	248
9.4.1 考点精讲	248
9.4.2 一点一练	254
9.4.3 解析与答案	255
9.5 网络系统建设	257
9.5.1 考点精讲	258
9.5.2 一点一练	260
9.5.3 解析与答案	261
9.6 考前冲刺	263
9.7 习题解析	266
第 10 章 网络管理技术	274
10.1 考点脉络	274
10.2 网络操作系统基本配置	274
10.2.1 考点精讲	274
10.2.2 一点一练	283
10.2.3 解析与答案	284
10.3 网管体系和故障诊断	287
10.3.1 考点精讲	287
10.3.2 一点一练	296
10.3.3 解析与答案	298
10.4 网管工具与网络存储	300
10.4.1 考点精讲	300
10.4.2 一点一练	305
10.4.3 解析与答案	306
10.5 考前冲刺	308
10.6 习题解析	311
第 11 章 网络安全技术	320
11.1 考点脉络	320
11.2 网络安全基础和计算机病毒	320
11.2.1 考点精讲	320
11.2.2 一点一练	324

11.2.3 解析与答案	325	12.3.1 考点精讲	361
11.3 加解密技术和认证技术	326	12.3.2 一点一练	371
11.3.1 考点精讲	326	12.3.3 解析与答案	372
11.3.2 一点一练	330	12.4 DHCP 服务	373
11.3.3 解析与答案	330	12.4.1 考点精讲	373
11.4 入侵检测系统与防火墙技术	331	12.4.2 一点一练	382
11.4.1 考点精讲	331	12.4.3 解析与答案	383
11.4.2 一点一练	335	12.5 Samba 和 Apache 服务器	384
11.4.3 解析与答案	336	12.5.1 考点精讲	384
11.5 电子商务与 VPN 技术	337	12.5.2 一点一练	390
11.5.1 考点精讲	337	12.5.3 解析与答案	391
11.5.2 一点一练	341	12.6 代理服务	392
11.5.3 解析与答案	342	12.6.1 考点精讲	392
11.6 考前冲刺	343	12.6.2 一点一练	395
11.7 习题解析	346	12.6.3 解析与答案	395
第 12 章 网络应用服务器配置	353	12.7 考前冲刺	397
12.1 考点脉络	353	12.8 习题解析	400
12.2 IIS 组件子服务配置	353	第 13 章 网络工程师案例分析	406
12.2.1 考点精讲	353	13.1 考点脉络	406
12.2.2 一点一练	358	13.2 考前冲刺	407
12.2.3 解析与答案	360	13.3 习题解析	414
12.3 DNS 服务	361		

计算机硬件基础是计算机从业人员必须要掌握的知识点，作为进入 IT 行业的入门知识点，是必须要学习的。

1.1 考点脉络

本章是网络工程师考试的一个必考点，根据考试大纲，要求考生掌握以下几个方面的内容。

- (1) 计算机组成：计算机的基本组成、CISC 和 RISC 特点、多处理机、总线和接口等。
- (2) 数据运算：数据的表示、逻辑运算。
- (3) 寻址方式：指令的各种寻址方式。
- (4) 中断：主要考查中断的概念，以及中断响应的过程。
- (5) 存储体系：内存编址、内存容量的计算、Cache（高速缓冲存储器）的计算。
- (6) 流水线：主要考查流水线概念、性能、有关参数计算等。
- (7) 性能评估：主要考查系统可靠性的计算、时钟频率等。

从历年的考试试题来看，本章的考点在综合知识考试中的平均分数为 4 分，约为总分的 5.33%。考试试题分数主要集中在计算机组成、数据运算、存储体系这 3 个知识点上。

1.2 计算机组成

在计算机组成这个考点中，主要涉及 4 个方面的知识，分别是计算机的基本组成、CISC 和 RISC 的特点、多处理机、总线和接口。

1.2.1 考点精讲

计算机基本组成重点讲述了计算机的硬件结构。RISC 和 CISC 是两种计算机指令系统体系。当前的高性能服务器与超级计算机大多具有多个处理机，能进行多任务处理，称为多处理机。总线和接口则介绍了总线与接口的分类和标准。

1. 计算机的基本组成

在一台计算机中，主要有 6 种部件，分别是控制器、运算器、内存储器、外存储器、输入设备和输出设备。它们之间的合作关系如图 1-1 所示。

其中控制器和运算器共同构成中央处理器（CPU）。CPU 主要通过总线和其他设备进行联系。另外在嵌入式系统设计中，外部设备也常常直接连接到 CPU 的外部 I/O 脚的中断脚上。

(1) 运算器

运算器的主要功能是在控制器的控制下完成各种算术运算、逻辑运算和其他操作。运算器主要包括算术逻辑单元（ALU）、加法器/累加器、数据缓冲寄存器、程序状态寄存器 4 个子部件构成。

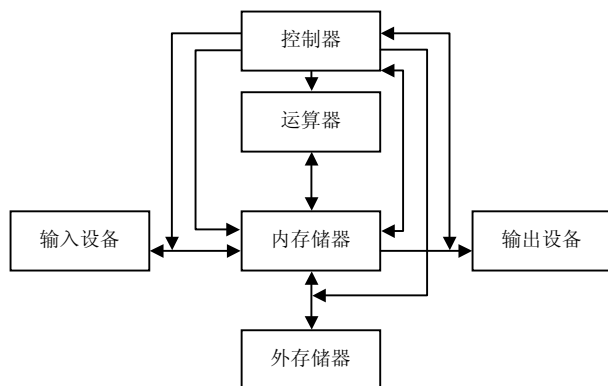


图 1-1 计算机各功能部件之间的合作关系

算术逻辑单元（ALU）主要完成对二进制数据的定点算术运算（加、减、乘、除）、逻辑运算（与、或、非、异或）以及移位操作。

累加寄存器（AC）通常简称为“累加器”，是一个通用寄存器。其功能是当运算器中的算术逻辑单元（ALU）执行算术或逻辑运算时为 ALU 提供一个工作区，用于传输和暂存用户数据。

数据缓冲寄存器用来暂时存放由内存器读出的一条指令或一个数据字。反之，当向内存存入一条指令或一个数据字时，也暂时将它们存放在数据缓冲寄存器中。数据缓冲寄存器的作用如下。

- ① 作为 CPU 和内存、外部设备之间信息传送的中转站。
- ② 补偿 CPU 和内存、外围设备之间在操作速度上的差别。
- ③ 在单累加器结构的运算器中，数据缓冲寄存器还可兼作操作数寄存器。

程序状态寄存器用来存放两类信息。一是体现当前指令执行结果的各种状态信息，如有无进位（CF 位）、有无溢出（OF 位）、结果正负（SF 位）、结果是否为零（ZF 位）和奇偶标志位（PF 位）等。二是控制信息，如允许中断（IF 位）和跟踪标志（TF 位）等。

(2) 控制器

控制器由程序计数器（PC）、指令寄存器、指令译码器、时序产生器和操作控制器组成，完成整个计算机系统的操作。

程序计数器（PC）是专用寄存器，具有存储和计数两种功能，又称为“指令计数器”。在程序开始执行前将程序的起始地址送入 PC，在程序加载到内存时以此地址为基础，因此 PC 的初始内容为程序第一条指令的地址。执行指令时 CPU 将自动修改 PC 的内容，以便使其保持的总是将要执行的下一条指令的地址。由于大多数指令都是按顺序执行，因此修改的过程通常只是简单地将 PC 加 1。当遇到转移指令时，后继指令的地址与前指令的地址加上一个向前或向后转移的位偏移量得到，或者根据转移指令给出的直接转移的地址得到。

指令寄存器存储当前正在被 CPU 执行的指令。

指令译码器将指令中的操作码解码，告诉 CPU 该做什么。可以说指令寄存器的输出内

容是指令译码器的输入内容。

时序产生器用以产生各种时序信号，以保证计算机能够准确、迅速、有条不紊地工作。

(3) 内存储器

内存储器又称内存或主存，用于存储现场操作的信息与中间结果，包括机器指令和数据。

(4) 外存储器

外存储器又称外存或辅助存储器 (Secondary Storage 或 Permanent Storage)，用于存储需要长期保存的各种信息。

(5) 输入设备 (Input Devices)

输入设备用以接收外界向计算机输入的信息。

(6) 输出设备 (Output Devices)

输出设备用以将计算机中的信息向外界输送。

2. RISC 和 CISC

随着硬件成本的下降，人们倾向于向中央处理器加入越来越多、越来越复杂的指令。同时，为了兼容老产品，原来的指令也要保留。这样，整个指令系统就向着越来越大、越来越复杂的趋势发展。在计算机处理能力越来越强的同时，中央处理器的设计也越来越复杂。这无疑大大增加了设计周期，更增加了设计失误的可能性。

另一方面，加大指令的复杂性和中央处理器功能的增加不一定是成正比的。人们发现许多方面存在一个二八定律，亦即系统中 20% 的组成部分发挥了 80% 的作用和功能，通过对复杂指令集计算机 (Complex Instruction Set Computer, CISC) 指令系统的研究，发现系统在 80% 的时间里执行 20% 的指令。

于是出现了精简指令的设计思想。这种计算机的指令结构不求最全面和复杂，而是只实现那些经常被执行的指令。由于指令的复杂性低很多，所以称为精简指令集计算机 (Reduced Instruction Set Computer, RISC)。

精简指令集计算机是相对于传统的复杂指令集计算机而言的。RISC 不是简单地把指令系统进行简化，而是通过简化指令的途径使计算机的结构更加简单合理，以减少指令的执行周期数，从而提高运算速度。

在这个知识点中，我们只需要了解 RISC 计算机的主要特点，列举如下。

(1) 指令数量少。优先选取使用频率最高的一些简单指令以及一些常用指令，避免使用复杂指令。大多数指令都是对寄存器操作，对存储器的操作仅提供了读和写这两种方式。

(2) 指令的寻址方式少。通常只支持寄存器寻址方式、立即数寻址方式以及相对寻址方式。

(3) 指令长度固定，指令格式种类少。因为 RISC 指令数量少，格式相对简单，其指令长度固定，指令之间各字段的划分比较一致，译码相对容易。

(4) 只提供了 Load/Store 指令访问存储器。只提供了从存储器读数 (Load) 和把数据写入存储器 (Store) 两条指令，其余所有的操作都在 CPU 的寄存器间进行。因此，RISC 需要大量的寄存器。

(5) 以硬布线逻辑控制为主。为了提高操作的执行速度，通常采用硬布线逻辑 (组合逻辑) 来构建控制器。而 CISC 的指令系统很复杂，难以用组合逻辑电路实现控制器，通常采用微程序控制。

(6) 单周期指令执行。因为简化了指令系统，很容易利用流水线技术使得大部分指令都能在一个机器周期内完成。因此，RISC 通常采用流水线组织。少数指令可能会需要多个周期执行，例如 Load/Store 指令因为需要访问存储器，其执行时间就会长一些。

(7) 优化的编译器。RISC 的精简指令集使编译工作简单化。因为指令长度固定、格式少、寻址方式少，编译时不必在具有相似功能的许多指令中进行选择，也不必为寻址方式的选择而费心，同时易于实现优化，从而可以生成高效率执行的机器代码。

大多数 RISC 采用了 Cache 方案，而且有的 RISC 甚至使用两个独立的 Cache 来改善性能。一个称为指令 Cache，另一个称为数据 Cache。这样取指令和读数据可同时进行，互不干扰。

从理论上来看，CISC 和 RISC 都有各自的优势，不能认为 RISC 就好，CISC 就不好。事实上，这两种设计方法很难找到完全的界线，而且在实际的芯片中，这两种设计方法也有相互渗透的地方，表 1-1 是两者的简单对比。

表 1-1 CISC 和 RISC 的简单对比

比 较 方 面	CISC	RISC
指令条数	多	只选取最常见的指令
指令复杂度	高	低
指令长度	变化	短、固定
指令执行周期	随指令变化大	大多在一个机器同期内完成
指令格式	复杂	简单
寻址方式	多	极少
涉及访问主存指令	多	极少，大部分只能存两条指令
通用寄存器数量	一般	大量
译码方式	微程序控制	硬件电路
对编译系统要求	低	高

3. 多处理机

本节主要介绍几种多处理机系统，对于多处理机这个知识点，了解即可。

(1) 超级标量处理机。在超级标量处理机中，配置了多个功能部件和指令译码电路，采取了多条流水线，还有多个寄存器端口和总线，因此可以同时执行多个操作，以并行处理来提高机器速度。它可以同时从存储器中取出几条指令同时送入不同的功能部件。超级标量处理机的硬件是不能重新安排指令的前后次序的，但可以在编译程序时采取优化的办法对指令的执行次序进行精心安排，把能并行执行的指令搭配起来。

(2) 超级流水线处理机。超级流水线处理机的周期比其他结构的处理机短。与超级标量处理机一样，硬件不能调整指令的执行次序，而由编译程序解决优先问题。

(3) 超长指令字处理机。超长指令字处理机是一种单指令流多操作码多数据的系统结构，编译程序在编译时把这个能并行执行的操作组合在一起，成为一条有多个操作段的超长指令，由这条超长指令控制计算机中多个互相独立的功能部件，每个操作段控制一个功能部件，相当于同时执行多条指令。

(4) 向量处理机。向量处理机是一种具有向量数据表示，并设置有相应的指令和硬件，能对向量的各个元素进行并行处理的计算机。当进行向量运算时，它的性能要比大型机好得多。向量处理机有巨型计算机和向量协处理机（也称为数组处理机）两种类型。巨型计算机能对大量的数据进行浮点运算，同时还是可以进行标量计算和一般数据处理的通用计算机。

向量处理机一般采用流水线工作,当它处理一条数组指令时,对数组中的每个元素执行相同的操作,而且各元素间是互相无关的,因此流水线不会阻塞,能以每个时钟周期送出一个结果的速度运行。为了存储系统能及时提供数据,向量处理机配有一个大容量的、分成多个模块交错工作的主存储器。为了提高运算速度,在向量处理机的运算部件中可采用多个功能部件,例如向量部件、浮点部件、整数运算部件和计算地址用的地址部件。向量处理机是专门处理浮点和向量运算的数组处理机,它连接到主机总线上。

(5) 多处理机系统。多处理机具有两个或两个以上的处理机,共享输入/输出子系统,在操作系统统一控制下,通过共享主存或高速通信网络进行通信,协同求解一个个复杂的问题。多处理机通过利用多台处理机进行多任务处理来提高速度,利用系统的重组能力来提高可靠性、适应性和可用性。多处理机具有共享存储器和分布存储器两种不同的结构。具有共享存储器的多处理机中,程序员无数据划分的负担,编程容易;系统处理机数目较少,不易扩充。具有分布式存储器的多处理机结构灵活,容易扩充;难以在各个处理单元之间实现复杂数据结构的数据传送;任务动态分配复杂;现有软件可继承性差,需要设计新的并行算法。多处理机系统属于 MIMD 系统,与 SIMD 的并行处理机相比,有很大的差别。其根源就在于两者的并行性的层次不同,多处理机要实现的是更高层次的作业任务间的并行。

(6) 大规模并行处理机。并行处理机也称为阵列处理机,并行处理机使用按地址访问的随机存储器,以 SIMD 方式工作,主要用于要求大量高速进行向量矩阵运算的应用领域。并行处理机制的并行性来源于资源重复,把大量相同的处理单元通过互联网络连接起来,在统一的控制器控制下,对各自分配来的数据并行地完成同一条指令所规定的操作。并行处理机有两种基本结构类型:采用分布存储器的并行处理结构和采用集中式共享存储器的并行处理结构。分布式存储器的并行处理结构中,每一个处理机都有自己局部的存储器,只要控制部件将并行处理的程序分配至各处理机,它们便能并行处理,各自从自己的局部存储器中取得信息。而共享存储器并行处理结构中的存储器是集中共享的,由于多个处理机共享,在各处理机访问共享存储器时会发生竞争。因此,需采取措施尽可能避免竞争的发生。大规模并行处理机(Massively Parallel Processor, MPP)是由众多的微处理器(从几百到上万)组成的大规模的并行系统。MPP 的出现成为计算机领域中一个研发热点,被用作开发万亿次甚至更高速的巨型机的主要结构。MPP 可以采用市场上出售的 RISC 处理器,所以有很高的性价比。

(7) 对称多处理机。对称多处理机(Symmetrical Multi Processor, SMP)目前也基于 RISC 微处理器。它与 MPP 最大的差别在于存储系统。SMP 有一个统一的共享主存空间,而 MPP 则是每个微处理器都拥有自己的本地存储器。

4. 总线和接口

总线就是一组进行互连和传输信息(指令、数据和地址)的信号线,它好比连接计算机系统各个部件之间的桥梁。另外,我们广义上通常也把 AGP 接口、USB 接口等称为 AGP 总线、USB 总线。可以说总线在计算机中无处不在。

(1) 总线的分类

按总线相对于 CPU 或其他芯片的位置可分为内部总线(Internal Bus)和外部总线(External Bus)两种。在 CPU 内部,寄存器之间和算术逻辑部件 ALU 与控制部件之间传输数据所用的总线称为内部总线;而外部总线是指 CPU 与内存 RAM、ROM 和输入/输出设备接口之间进行通信的通路。由于 CPU 通过总线实现程序取指令、内存/外设的数据交换,在 CPU 与外设一定的情况下,总线速度是制约计算机整体性能的最大因素。

按总线功能来划分又可分为地址总线、数据总线、控制总线 3 类。我们通常所说的总线

都包括上述 3 个组成部分，地址总线用来传送地址信息，数据总线用来传送数据信息，控制总线用来传送各种控制信号。例如 ISA 总线共有 98 条线，其中数据线 16 条，地址线 24 条，其余为控制信号线、接地线和电源线。

按总线在微机系统中的位置可分为机内总线和机外总线两种。我们上面所说的总线都是机内总线，而机外总线是指与外部设备接口相连的，实际上是一种外设的接口标准。如计算机上的接口标准 IDE、SCSI、USB 和 IEEE 1394 等，前两种主要是与硬盘、光驱等 IDE 设备接口相连，后两种新型外部总线可以用来连接多种外部设备。

计算机的总线按其功用来划分主要有局部总线、系统总线、通信总线 3 种类型。其中局部总线是在传统的 ISA 总线和 CPU 总线之间增加的一级总线或管理层，它的出现是由于计算机软、硬件功能的不断发展，系统原有的 ISA/EISA 等已远远不能适应系统高传输能力的要求，而成为整个系统的主要瓶颈。系统总线是计算机系统内部各部件（插板）之间进行连接和传输信息的一组信号线，例如 ISA、EISA、MCA、VESA、PCI、AGP 等。通信总线是系统之间或微机系统与设备之间进行通信的一组信号线。

（2）总线的标准

总线标准是指计算机部件各生产厂家都需要遵守的系统总线要求，从而使不同厂家生产的部件能够互换。总线标准主要规定总线的机械结构规范、功能结构规范和电气规范。总线标准可以分为正式标准和工业标准，其中正式标准是由 IEEE 等国际组织正式确定和承认的标准；工业标准是首先由某一厂家提出，得到其他厂家广泛使用的标准。

（3）接口的分类

根据外部设备与 I/O 模块交换数据的方式，系统接口可以分为串行接口和并行接口两种。串行接口一次只能传送 1 位信息，而并行接口一次就可传送多位信息（一般为 8 的倍数）。串行通信又分为异步通信方式和同步通信方式两种。并行接口数据传输速率高，控制简单，通常用于高速数据通道接口。但是所需连线很多，不适于远距离传送。串行通信连线少，适于长距离传送。但是控制复杂而且传输速度较慢。

（4）常见接口

常见的设备接口有以下几种。

① ST506：主要用于温盘，结构简单，只完成磁盘信息的读/写放大，把数据的编码解码、数据的格式转换等功能都留给 I/O 模块处理。其传输速率为 5~7Mb/s，最多可支持 2 个硬盘，最大支持盘空间为 150MB。

② ESDI：一种通用的标准接口，不仅适用于小型温盘，还适用于磁带机和光盘存储器。该接口除了完成信息的读/写放大外，还要完成数据的编码解码。数据传输速率为 5~10Mb/s，最多可支持 4 个硬盘，硬盘空间最大可达 600MB。

③ IDE：IDE 是最常用的磁盘接口，分为普通 IDE 和增强型 IDE（EIDE）接口。普通 IDE 数据传输速率不超过 1.5Mb/s，数据传输宽度为 8 位，最多可连接 4 个 IDE 设备，每个 IDE 硬盘容量不超过 528MB。根据传输速率的不同，EIDE 可以分为 UDMA-33、UDMA-66、UDMA-133 三类，数据传输速率可达 12~18Mb/s，数据传输宽度为 32 位，最多可连接 4 个 IDE 设备，每个 IDE 硬盘可超过 528MB。

④ SCSI：数据宽度为 8 位、16 位和 32 位，是大容量存储设备、音频设备和 CD-ROM 驱动器的一种标准。SCSI 接口通常被看作一种总线，可用于连接多个外设，这些 SCSI 设备以雏菊链（Mode Daisy Chain）形式接入，并被分配给唯一的 ID 号（0~7），其中 7 号分配给 SCSI 控制器。某些 SCSI 控制器可以提供多达 35 个 SCSI 通道。SCSI 设备彼此独立运作，

最初的 SCSI 标准（目前又称为 SCSI I）的最大同步传输速率为 5Mb/s，后来的 SCSI II 规定了 2 种提高速度的选择。一种为提高数据传输的频率，即“Fast SCSI”。由于频率提高了一倍，即使数据通路仍和 SCSI II 同为 8 位宽，其最大同步传输速率也提高了一倍，达到 10Mb/s。另一种提高速度的选择是传输频率提高一倍的同时也增大数据通路的宽度，由 8 位增至 16 位，这就是“Wide SCSI”，其最大同步传输速率为 20Mb/s。

⑥ **P1394:** P1394 是一种高速的串行总线，用于连接众多的外部设备。P1394 有许多优于 SCSI 等其他外设接口的特点，如数据传输速率高，价格低且容易实现，所以不仅应用于计算机系统中，也广泛应用于消费类电子产品中，诸如数码相机、VCD 等。P1394 的数据传输速率可达 400Mb/s，新的标准是 800Mb/s。P1394 接口使用雏菊链式的设备连接方式，一个端口可以支持 63 个设备；而且使用桥互联的方式，以树型结构配置，可以支持的设备数高达 1022。P1394 支持设备的热插拔，即允许计算机在未关机带电的情况下插入或拔除所连接的外部设备而不会造成损害。

⑦ **USB:** USB 接口是一种串行总线式的接口，在串行接口中可达到较高的数据传输速率，并且也允许设备以菊花链形式接入，最多可连接 127 个设备。USB 的最大特点是允许热插拔，目前在便携式计算机和台式计算机中已成为标准配置。许多数码相机、闪存、视频摄像头以及打印机等都可通过 USB 口接入计算机。USB 1.0 的速度是 1.2Mb/s，USB 2.0 的速度达到了 480Mb/s，USB 3.0 的速度达到了 5Gb/s。

(1) A. 地址寄存器 (MAR) B. 数据寄存器 (MDR)
C. 程序计数器 (PC) D. 指令寄存器 (IR)

(2) A. 操作码应存入指令寄存器 (IR), 地址码应存入程序计数器 (PC)
B. 操作码应存入程序计数器 (PC), 地址码应存入指令寄存器 (IR)
C. 操作码和地址码都应存入指令寄存器 (IR)
D. 操作码和地址码都应存入程序计数器 (PC)

(3) A. 提高数据传输速度 B. 提高数据传输量
C. 减少信息传输线的数量 D. 减少指令系统的复杂性

第 1 章 计算机硬件基础 7

或者存放从存储器读取的数据以及写入存储器的数据的寄存器。

地址寄存器用来保存当前 CPU 所访问的内存单元的地址。由于在内存和 CPU 之间存在着操作速度上的差别，所以必须使用地址寄存器来保持地址信息，直到内存的读/写操作完成为止。

试题 1 答案

(1) C

试题 2 分析

这是一道基础概念题，考查 IR 及 PC 等基本寄存器的作用。PC 用于存放 CPU 下一条要执行的指令地址，在顺序执行程序当中其内容送到地址总线后会自动加 1，指向下一条将要运行的指令地址；IR 用来保存当前正在执行的一条指令，而指令一般包括操作码和地址码两部分，因此这两部分均存放在 IR 中。

试题 2 答案

(2) C

试题 3 分析

采用总线结构的主要优点有：总线是计算机中各部件相连的传输线，通过总线，各部件之间可以相互通信，而不是每两个部件之间相互直连，减少了计算机体系结构的设计成本，有利于新模块的扩展。

试题 3 答案

(3) C

试题 4 分析

CPU 即中央处理单元，是整个计算机控制中心，由运算器、控制器、寄存器组和一些内部总线组成。控制器有程序计数器、指令寄存器、指令译码器、时序产生器和操作控制器组成，完成指挥整个计算机系统的操作。其基本功能包括在内存中去除一条指令并指出下一条指令的位置、对指令进行译码产生相应的控制信号完成规定的动作，以及控制各种设备之间数据的流动。

PC 是专用寄存器，具有存储和计数两种功能，又称为“指令计数器”。在程序开始执行前将程序的起始地址送入 PC，在程序加载到内存时以此地址为基础，因此 PC 的初始内容即程序第 1 条指令的地址。执行指令时 CPU 将自动修改 PC 的内容，一般使其保存的总是将要执行的下一条指令的地址。由于大多数指令都是按照顺序执行，因此，修改的过程通常只是简单地将 PC 加 1。当遇到转移指令时后继指令的地址与前指令的地址加上一个向前或向后转移的位移量得到，或者根据转移指令给出的直接转移地址得到。

试题 4 答案

(4) B

试题 5 分析

本题主要考查寄存器的相关内容。

程序计数器是用于存放下一条指令所在单元的地址的地方。在程序执行前，必须将程序的起始地址，即程序的一条指令所在的内存单元地址送入程序计数器，当执行指令时，CPU 将自动修改程序计数器的内容，即每执行一条指令程序计数器增加一个量，使其指向下一个待执行的指令。程序的转移等操作也是通过该寄存器来实现的。

地址寄存器一般用来保存当前 CPU 所访问的内存单元的地址，以方便对内存的读/写操作。

累加器是专门存放算术或逻辑运算的一个操作数和运算结果的寄存器。ALU 是 CPU 的执行单元，主要负责运算工作。

试题 5 答案

(5) A

试题 6 分析

本题考查的是计算机系统硬件方面的基础知识。构成计算机控制器的硬件主要有指令寄存器 IR、程序计数器 PC、程序状态字寄存器 PSW、时序部件和微操作形成部件等。而算术逻辑单元 ALU 不是构成控制器的部件。

试题 6 答案

(6) C

试题 7 分析

本题考查的是 RISC 设计方面的基础知识。在设计 RISC 时，需要遵循如下一些基本的原则。

- ① 指令条数少，一般为几十条指令。
- ② 寻址方式尽可能少。
- ③ 用等长指令，不管功能复杂的指令还是简单的指令，均用同一长度。
- ④ 设计尽可能多的通用寄存器。

因此，采用“变长指令，功能复杂的指令长度长而简单指令长度短”不是应采用的设计原则。

试题 7 答案

(7) C

试题 8 分析

本题考查寄存器的类型和特点。

寄存器是 CPU 中的一个重要组成部分，它是 CPU 内部的临时存储单元。寄存器既可以用来存放数据和地址，也可以存放控制信息或 CPU 工作时的状态。在 CPU 中增加寄存器的数量，可以使 CPU 把执行程序时所需的数据尽可能地放在寄存器中，从而减少访问内存的次数，提高其运行速度。但是，寄存器的数目也不能太多，除了增加成本外，由于寄存器地址编码增加也会相对增加指令的长度。CPU 中的寄存器通常分为存放数据的寄存器、存放地址的寄存器、存放控制信息的寄存器、存放状态信息的寄存器等类型。

程序计数器用于存放指令的地址。令当程序顺序执行时，每取出一条指令，PC 内容自动增加一个值，指向下一条要取的指令。当程序出现转移时，则将转移地址送入 PC，然后由 PC 指向新的程序地址。

程序状态寄存器用于记录运算中产生的标志信息，典型的标志为有进位标志位、0 标志位、符号标志位、溢出标志位和奇偶标志位等。

地址寄存器包括程序计数器、堆栈指示器、变址寄存器和段地址寄存器等，用于记录各种内存地址。

累加寄存器是一个数据寄存器，在运算过程中暂时存放被操作数和中间运算结果，累加器不能用于长时间地保存一个数据。

试题 8 答案

(8) B

试题 9 分析

本题考查计算机系统总线和接口方面的基础知识。

广义地讲,任何连接两个以上电子元器件的导线都可以称为总线。通常可分为 4 类:

- ① 芯片内总线。用于在集成电路芯片内部各部分的连接。
- ② 元件级总线。用于一块电路板内各元器件的连接。
- ③ 内总线,又称系统总线。用于构成计算机各组成部分(CPU、内存和接口等)连接。
- ④ 外总线,又称通信总线。用计算机与外设或计算机与计算机的连接或通信。

连接处理机的处理器、存储器及其他部件的总线属于内总线,按总线上所传送的内容分为数据总线、地址总线和控制总线。

试题 9 答案

(9) A

试题 10 分析

本题考查指令系统和计算机体系结构基础知识。

复杂指令集计算机(Complex Instruction Set Computer, CISC)的基本思想是:进一步增强原有指令的功能,用更为复杂的新指令取代原先由软件子程序完成的功能,实现软件功能的硬件化,导致机器的指令系统越来越庞大和复杂。CISC 计算机一般所含有的指令数目至少 300 条以上,有的甚至超过 500 条。

精简指令集计算机(Reduced Instruction Set Computer, RISC)的基本思想是:通过减少指令总数和简化指令功能,降低硬件设计的复杂度,使指令能单周期执行,并通过优化编译提高指令的执行速度,采用硬布线控制逻辑优化编译程序。在 20 世纪 70 年代末开始兴起,导致机器的指令系统进一步精炼而简单。

试题 10 答案

(10) A

1.3 数据运算

对于本知识点的考查,主要是数据的各种码制的表示和逻辑运算两个方面的内容。

1.3.1 考点精讲

码制和逻辑运算都是计算机科学基础中重要的组成部分。对于逻辑运算而言在考试中虽然没有专门的考试真题,但诸如海明校验是需要用到逻辑运算这个知识点的。

1. 各种码制

本节主要掌握原码、反码、补码和移码的概念,以及各自的用途和优缺点。

(1) 原码

将最高位用作符号位(0 表示正数,1 表示负数),其余各位代表数值本身的绝对值的表示形式。这种方式是最容易理解的。例如,假设用 8 位表示一个数,则+11 的原码用二进制表示是 00001011, -11 的原码用二进制表示是 10001011。

直接使用原码在计算时会有麻烦。例如,在十进制中 $1+(-1)=0$ 。如果直接使用二进制原码来执行“ $1+(-1)$ ”的操作,则表达式为: $00000001+10000001=10000010$

这样计算的结果是-2,也就是说,使用原码直接参与计算可能会出现错误的结果。所以,原码的符号位不能直接参与计算,必须和其他位分开,这样会增加硬件的开销和复杂性。

(2) 反码

正数的反码与原码相同。负数的反码符号位为 1，其余各位为该数绝对值的原码按位取反。例如，-11 的反码为 11110100。

同样，对于“1+(-1)”加法，使用反码的结果是：

$$00000001+11111110=11111111$$

这样的结果是负 0，而在人们普遍的观念中，0 是不分正负的。反码的符号位可以直接参与计算，而且减法也可以转换为加法计算。

(3) 补码

正数的补码与原码相同。负数的补码是该数的反码加 1，这个加 1 就是“补”。例如，-11 的补码为：

$$11110100+1=11110101$$

对于“1+(-1)”的加法，是这样的：

$$00000001+11111111=00000000$$

这说明，直接使用补码进行计算的结果是正确的。

对一个补码表示的数，要计算其原码，只要对它再次求补即可。由于补码能使符号位与有效值部分一起参加运算，从而简化了运算规则，同时它也使减法运算转换为加法运算，进一步简化计算机中运算器的电路，这使得在大部分计算机系统中，数据都使用补码表示。

(4) 移码

移码又称为增码，移码的符号表示和补码相反，1 表示正数，0 表示负数。也就是说，移码是在补码的基础上把首位取反得到的，这样使得移码非常适合于阶码的运算，所以移码常用于表示阶码。

通过 4 种码制的学习，我们已经学会了它们相互之间的转换。当要面临着取值范围时，请参照表 1-2。

表 1-2 各种码制取值范围

名 称	定 点 整 数	定 点 小 数
原码	$-(2^{n-1}-1) \sim 2^{n-1}-1$	$-1 < X < 1$
反码	$-(2^{n-1}-1) \sim 2^{n-1}-1$	$-1 < X < 1$
补码	$-2^{n-1} \sim 2^{n-1}-1$	$-1 \leq X < 1$

2. 逻辑运算

在计算机中，运算可以分为算术运算和逻辑运算。二进制数 1 和 0 在逻辑上可以代表“真”与“假”、“是”与“否”、“有”与“无”。这种具有逻辑属性的变量就称为逻辑变量，逻辑变量之间的运算称为逻辑运算。

逻辑运算与算术运算的主要区别是：逻辑运算是按位进行的，位与位之间不像加、减运算那样有进位或借位的联系。

逻辑运算主要包括 4 种基本运算，分别是逻辑加法（或运算）、逻辑乘法（与运算）、逻辑否定（非运算、否运算）和异或运算（半加运算）。

(1) 逻辑加法

逻辑加法通常用符号“+”或“∨”来表示。逻辑加法运算规则如下：

$$0+0=0, 0\vee 0=0$$

$$0+1=1, 0\vee 1=1$$

$$1+0=1, 1\vee 0=1$$

$$1+1=1, 1\vee 1=1$$

对于逻辑加法,在给定的逻辑变量 A 和 B 中,只要有一个为 1,其逻辑加的结果就为 1。只有两者都为 0 时,逻辑加的结果才为 0。

(2) 逻辑乘法

逻辑乘法通常用符号“ \times ”或“ \wedge ”或“ \cdot ”来表示。逻辑乘法运算规则如下:

$$0\times 0=0, 0\wedge 0=0, 0\cdot 0=0$$

$$0\times 1=0, 0\wedge 1=0, 0\cdot 1=0$$

$$1\times 0=0, 1\wedge 0=0, 1\cdot 0=0$$

$$1\times 1=1, 1\wedge 1=1, 1\cdot 1=1$$

对于逻辑乘法,当参与运算的逻辑变量都同时取值为 1 时,其逻辑乘积才等于 1。只要有一个逻辑变量为 0,其结果就为 0。

(3) 逻辑否定

逻辑非的规则为把变量取反,即:

$$\bar{0}=1, \bar{1}=0$$

(4) 异或运算

异或运算通常用符号“ \oplus ”表示,其运算规则为:

$$0\oplus 0=0, 0\oplus 1=1, 1\oplus 0=1, 1\oplus 1=0$$

也就是说,只有两个逻辑变量相异(一个为 0,另一个为 1),结果才为 1。如果两个逻辑变量相同,则结果为 0。

1.3.2 一点一练

试题 1

某机器的字长为 8,符号位占 1 位,数据位占 7 位,采用补码表示时的最小整数为(1)。

- (1) A. -2^8 B. -2^7 C. -2^7+1 D. -2^8+1

试题 2

计算机中, (2)。

- (2) A. 指令和数据都是采用十进制存储
B. 指令和数据都是采用二进制存储
C. 指令用十进制存储,数据采用二进制存储
D. 指令用二进制存储,数据采用十进制存储

试题 3

在(3)表示中,数值 0 是唯一表示的。

- (3) A. 原码 B. 反码 C. 补码 D. 原码或反码

试题 4

若用 8 位机器码表示十进制数-101,则原码表示的形式为(4);补码表示的形式

为 (5)。

- (4) A. 11100101 B. 10011011 C. 11010101 D. 11100111
(5) A. 11100101 B. 10011011 C. 11010101 D. 11100111

试题 5

某逻辑电路有两个输入端分别为 X 和 Y，其输出端为 Z。当且仅当两个输入端 X 和 Y 同时为 0 时，输出端 Z 才为 0，则该电路输出端 Z 的逻辑表达式为 (6)。

- (6) A. $X \cdot Y$ B. $\overline{X \cdot Y}$ C. $X \oplus Y$ D. $X + Y$

试题 6

在进行定点原码乘法运算时，乘积的符号位是被乘数的符号位和乘数的符号位 (7) 运算来获得。

- (7) A. 相或 B. 相与
C. 相异或 D. 分别取反后再相或

试题 7

若操作数“00000101”与“00000101”执行逻辑 (8) 操作后结果为“00000000”。

- (8) A. 或 B. 与 C. 异或 D. 与非

试题 8

用补码表示的 8 位二进制数 11100000 的值为十进制数 (9)。

- (9) A. -31 B. -32 C. -64 D. -65

试题 9

两个带符号的数进行运算时，在 (10) 的情况下有可能产生溢出。

- (10) A. 同符号数相加 B. 同符号数相减
C. 异符号数相加 D. 异符号数相或

试题 10

欲知 8 位二进制数 ($b_7b_6b_5b_4b_3b_2b_1b_0$) 的 b_2 是否为 1，可将该数与二进制数 00000100 进行 (11) 运算，若运算结果不为 0，则此数的 b_2 必为 1。

- (11) A. 加 B. 减 C. 与 D. 或

1.3.3 解析与答案

试题 1 分析

对于原码、反码、补码，假设用 n 位表示数据（二进制数），则各种表示方法的表示范围如表 1-3 所示。

表 1-3 各种码制取值范围

名 称	定 点 整 数	定 点 小 数
原码	$-(2^{n-1}-1) \sim 2^{n-1}-1$	$-1 < X < 1$
反码	$-(2^{n-1}-1) \sim 2^{n-1}-1$	$-1 < X < 1$
补码	$-2^{n-1} \sim 2^{n-1}-1$	$-1 \leq X < 1$

试题 1 答案

- (1) B

试题 2 分析

在计算机中，所有的数据或信息都是采用二进制存储的。使用二进制主要有以下优点：

① 电路中更容易实现。二进制只有 0 和 1，那么电路只要能识别低和高电平即可表示 0 和 1。

② 易于实现物理存储。

③ 便于进行加减运算和计算编码。

④ 便于逻辑判断（是或非）。

⑤ 用二进制表示数据具有抗干扰能力强、可靠性高的优点。

试题 2 答案

(2) B

试题 3 分析

将最高为作符号位（0 表示正数，1 表示负数），其余各位代表数值本身绝对值的表现形式称为原码表示。在原码机器中往往有“+0”和“-0”之分， $[+0]_{\text{原}}=0.00\cdots 0$ ， $[-0]_{\text{补}}=1.00\cdots 0$ 。反码就是原码的各位数（除符号位外）码 0 变为 1，1 变为 0；对于 0，有 $[+0]_{\text{反}}=[+0]_{\text{原}}$ ， $[+0]_{\text{反}}=0.00\cdots 0$ ， $[-0]_{\text{反}}=1.11\cdots 1$ 。补码是在反码的基础上加 1，对于 0， $[+0]_{\text{补}}=[+0]_{\text{原}}$ ， $[+0]_{\text{补}}[-0]_{\text{补}}=0.0000000=[+0]_{\text{补}}$ ，即 0 的补码表示形式是唯一的。

试题 3 答案

(3) C

试题 4 分析

将最高为作符号位（0 表示正数，1 表示负数），其余各位代表数值本身的绝对值的表现形式称为原码表示。因此，-101 的原码是 111000101。

正数的补码与原码相同，负数的补码为该数的反码加 1。正数的反码与原码相同，负数的反码符号位为 1，其余各位为该数绝对值的原码按位取反。-101 的原码是 11100101，反码为 10011010，则其补码为 10011011。

试题 4 答案

(4) A

(5) B

试题 5 分析

$X \cdot Y$ 表示逻辑与，其特点是只有两个或多个输入全部为 1 时，其结果才为 1，即两个输入相异时即为 0 时，其输出即为 0。

$X + Y$ 表示逻辑或，其特点是两个或多个输入中只要有一个位 1，则结果为 1；只有当两个输入都为 0 时，其输出才为 0。

$X \oplus Y$ 表示逻辑异或，其特点是半加法。当 1 和 0 做异或运算时结果为 1，0 与 0 或者 1 与 1 作异或运算时，其结果为 0。

试题 5 答案

(6) D

试题 6 分析

根据原码 1 位乘法的法则，应当是被乘数的符号位和乘数的符号位相异或作为乘积的符号位。

试题 6 答案

(7) C

试题 7 分析

逻辑代数的三种最基本的运算为“与”、“或”、“非”运算。

“与”运算又称为逻辑乘，其运算符号常用 AND、 \cap 、 \wedge 或 \cdot 表示。设 A 和 B 为两个逻辑变量，当且仅当 A 和 B 的取值都为“真”时，A “与” B 的值为“真”；否则 A “与”的值为“假”。操作数“00000101”与“00000101”执行逻辑“与”后的结果为“00000101”。

“或”运算也称为逻辑加，其运算符号常用 OR、 \cup 、 \vee 或 + 表示。设 A 和 B 为两个逻辑变量，当且仅当 A 和 B 的取值都为“假”时，A “或” B 的值为“假”；否则 A “或” B 的值为“真”。操作数“00000101”与“00000101”执行逻辑或后的结果为“00000101”。

“非”运算也称为逻辑求反运算，常用表示对变量 A 的值求反。其运算规则很简单：“真”的反为“假”，“假”的反为“真”。

“异或”运算又称为半加法运算，其运算符号常用 XOR 或表示。设 A 和 B 为两个逻辑变量，当且仅当 A、B 的值不同时，A “异或” B 为真。A “异或” B 的运算可由前三种基本运算表示。操作数“00000101”与“00000101”执行逻辑“异或”后的结果为“00000000”。

“与非”运算指先对两个逻辑量求“与”，然后对结果再求“非”。操作数“00000101”与“00000101”执行逻辑“与非”后的结果为“11111010”。

试题 7 答案

(8) C

试题 8 分析

根据原码与补码的转换规则，即正数的补码即原码本身，而负数的补码则是在原码的基础上，对其各位进行取反（最高位符号位除外），最后加 1。如果已知某数的补码，可能通过相同的步骤，即再一次取反加 1，就得到它的原码。题中，补码为：11100000，可以将其再次“取反加 1”，可得到二进制数为：10100000，最高位符号位是 1，表示它是负数，则表示是正数，即：-32。

试题 8 答案

(9) B

试题 9 分析

如果认为 a 和 b 都是有符号数，那么判断方法如下。

判断 a+b 是否溢出（超过有符号数的表示范围）的方法是：a，b 符号位不同，无溢出；a，b 符号位相同，并且计算结果的符号位也相同，无溢出，否则溢出。

判断 a-b 是否溢出（超过有符号数的表示范围）的方法是：a，b 符号位相同，无溢出；a，b 符号位不同，用判断 a+b 是否溢出的方法判断。

试题 9 答案

(10) A

试题 10 分析

这里只要了解二进制数运算的几个概念，很容易分析出，要想结果必定不为 0，并且原数中的第三位是 1，只有“与”运算满足条件，“与”运算只对位进行操作，不涉及进位，它的描述是“真真为真”，即 1，否则为假，即 0。

试题 10 答案

(11) C

1.4 存储体系与寻址方式

存储体系是计算机系统中非常重要的一个部分。在存储体系这个考点中，主要涉及主存、高速缓存、寻址方式三个方面的内容。

1.4.1 考点精讲

主存又称为内存，需要考生熟悉其分类和编制。高速缓存也就是 Cache，是介于 CUP 与存储体系之间一个非常重要的部件。RAID 是多台磁盘存储器组成的一个快速、大容量高可靠性的辅助存储子系统。寻址方式这一知识点，近几年考试出现的几率较小，对其寻址的种类了解即可。

1. 存储器的存取方式

(1) 存储器的基本存取方式

存储器的基本存取方式如表 1-4 所示。

表 1-4 存储器的基本存取方式

存取方式	读/写装置	数据块标志	访问特性	代表
顺序存取	共享读/写装置	无	特定线性顺序	磁带
直接存取	共享读/写装置	数据分块，每块一个唯一标志	可直接移到特定数据块	磁盘
随机存取	每个可寻址单元专用读/写装置	每个可寻址单元均有一个唯一地址	随时访问任何一个存储单元	主存储器
相连存取（属随机存取）	每个可寻址单元专用读/写装置	每个可寻址单元均有一个唯一地址	根据内容而非地址来选读/写点	Cache

(2) 存储器的性能

存取时间：对于随机存取而言，就是完成一次读/写所花的时间；对非随机存取而言，就是将读/写装置移动到目的位置所花的时间。

存储器带宽：每秒钟能访问的位数。通常存储器周期是纳秒级（ns，即 10^{-9} s）的，因此通常情况下的计算公式是： $1/\text{存储器周期} \times \text{每周期可访问的字节数}$ 。例如：存储器周期是 200ns，而每个周期可访问 4B，则带宽= $1\text{s}/200\text{ns} \times (4\text{B} \times 8) = 160\text{Mb/s}$ 。

数据传输率：每秒钟输入/输出的数据位数。对于随机存取而言，传输率 $R=1/\text{存储器周期}$ ；对于非随机存取而言，读/写 N 位所需的平均时间= $\text{平均存取时间}+N \text{ 位}/\text{数据传输率}$ 。

2. 主存储器基础

(1) 主存储器的种类

- ① RAM：随机存储器，可读/写，断电后数据无法保存，只能暂存数据。
- ② SRAM：静态随机存储器，在不断电时信息能够一直保持。
- ③ DRAM：动态随机存储器，需要定时刷新以维持信息不丢失。
- ④ ROM：只读存储器，出厂前用掩膜技术写入，常用于存放 BIOS 和微程序控制。
- ⑤ PROM：可编程 ROM，只能够一次写入，需用特殊电子设备进行写入。
- ⑥ EPROM：可擦除的 PROM，用紫外线照射 15~20 分钟可擦去所有信息，可写入多次。
- ⑦ E²PROM：电可擦除 EPROM，可以写入，但速度慢。
- ⑧ 闪存存储器：现在 U 盘使用的种类，可以快速写入。

记忆时，抓住几个关键英文字母。A，即 Access，说明读/写都行；O，即 Only，说明只读；P，即 Programmable，说明可通过特殊电子设备写入；E，即 Erasable，说明可擦写；E 平方说明是两个 E，第二个 E 是指电子。

(2) 主存储器的组成

实际的存储器总是由一片或多片存储器配以控制电路构成的。其容量为 $W \times B$ ， W 是存储单元（word，即字）的数量， B 表示每个 word 由多少 bit（位）组成。如果某一芯片规格为 $w \times b$ ，则组成 $W \times B$ 的存储器需要用 $(W/w) \times (B/b)$ 个芯片，如图 1-2 所示。

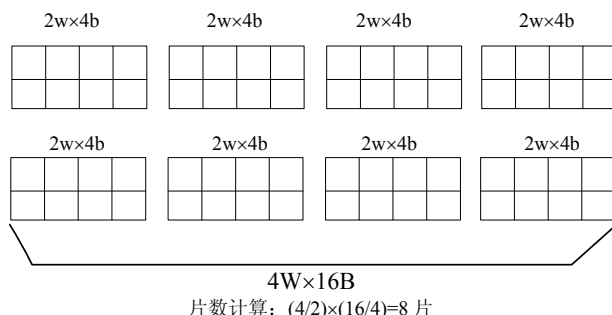


图 1-2 主存储器的组成示意图

(3) 主存储器的地址编码

主存储器（内存）采用的是随机存取方式，需对每个数据块进行编码，而在主存储器中，数据块是以 word 为单位来标识的，即每个字一个地址，通常采用的是十六进制表示。

例如，按字节编址，地址从 A4000H~CBFFFH，则表示有 $(CBFFF - A4000 + 1)$ 字节，即 28000H 字节，也就是 163 840 字节，等于 160KB。

要注意的是，编址的基础可以是字节，也可以是字（字是由 1 个或多个字节组成的），要算地址位数，首先应计算要编址的字或字节数，然后求 2 的对数即可得到。例如，上述内存的容量为 160KB，则需要 18 位地址来表示 $(2^{17} = 131\,072, 2^{18} = 262\,144)$ 。

关于内存这个知识点的另外一个问题就是求存储芯片的组成问题。实际的存储器总是由一片或多片存储器配以控制电路构成的。设其容量为 $W \times B$ ， W 是存储单元的数量， B 表示每个单元由多少位组成。如果某一芯片规格为 $w \times b$ ，则组成 $W \times B$ 的存储器需要用 $(W/w) \times (B/b)$ 块芯片。例如，上述例子中的存储器容量为 160KB，若用存储容量为 32K×8bit 的存储芯片构成，因为 $1B = 8b$ （一字节由 8 位组成），则至少需要 $(160K/32K) \times (1B/8b) = 5$ 块。

3. 高速缓冲存储器

Cache 的功能是提高 CPU 数据输入/输出的速率，突破所谓的“冯·诺依曼瓶颈”，即 CPU 与存储系统间数据传送带宽限制。高速存储器能以极高的速率进行数据的访问，但因其价格高昂，如果计算机的内存完全由这种高速存储器组成，则会大大增加计算机的成本。通常在 CPU 和内存之间设置小容量的高速存储器 Cache。Cache 容量小但速度快，内存速度较低但容量大，通过优化调度算法，系统的性能会大大改善，其存储系统容量与内存相当而访问速度近似 Cache。

(1) Cache 原理、命中率、失效率

使用 Cache 改善系统性能的主要依据是程序的局部性原理。通俗地说，就是一段时间内，执行的语句常集中于某个局部。而 Cache 正是通过将访问集中的内容放在速度更快的 Cache

上来提高性能的。引入 Cache 后, CPU 在需要数据时, 先找 Cache, 没找到再到内存中找。

如果 Cache 的访问命中率为 h (通常 $1-h$ 就是 Cache 的失效率), 而 Cache 的访问周期时间是 t_1 , 主存储器的访问周期时间是 t_2 , 则整个系统的平均访存时间就应该是:

$$t_3 = h \times t_1 + (1-h) \times t_2$$

从公式可以看出, 系统的平均访存时间与命中率有很密切的关系。灵活地应用这个公式, 可以计算出所有情况下的平均访存时间。

例如, 假设某流水线计算机主存的读/写时间为 100ns, 有一个指令和数据合一的 Cache, 已知该 Cache 的读/写时间为 10ns, 取指令的命中率为 98%, 取数据的命中率为 95%。在执行某类程序时, 约有 1/5 指令需要存/取一个操作数。假设指令流水线在任何时候都不阻塞, 则设置 Cache 后, 每条指令的平均访存时间约为多少? 其实这是应用公式的一道简单数学题:

$$(2\% \times 100\text{ns} + 98\% \times 10\text{ns}) + 1/5 \times (5\% \times 100\text{ns} + 95\% \times 10\text{ns}) = 14.7\text{ns}$$

(2) Cache 存储器的映射机制

分配给 Cache 的地址存放在一个相连存储器 (CAM) 中。CPU 发生访存请求时, 会让 CAM 判断所要访问的字的地址是否在 Cache 中, 如果命中就直接使用。这个判断的过程就是 Cache 地址映射, 这个速度应该尽可能快。常见的映射方法有直接映射、全相联映射和组相联映射三种, 其原理如图 1-3 所示。

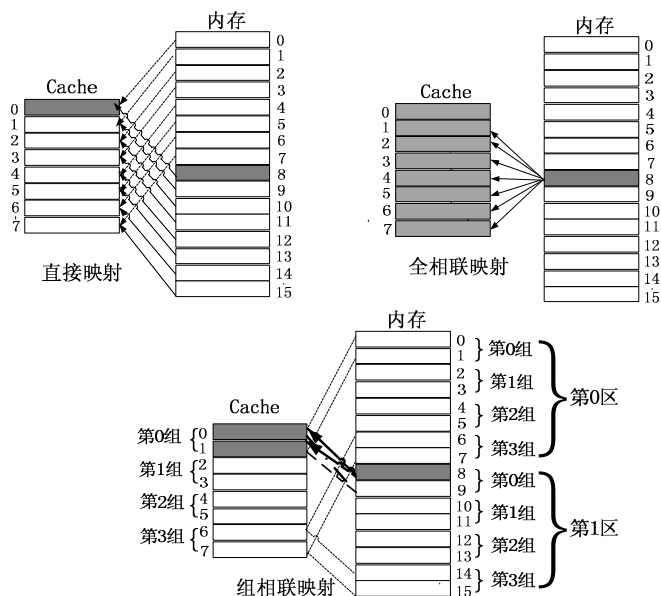


图 1-3 常见的 Cache 映射方法原理

① 直接映射: 是一种多对一的映射关系, 但一个主存块只能够复制到 Cache 的一个特定位置上去。Cache 的行号 i 和主存的块号 j 有函数关系: $i = j \% m$ (其中 m 为 Cache 总行数)。

例如, 某 Cache 容量为 16KB (即可用 14 位表示), 每行的大小为 16B (即可用 4 位表示), 则说明其可分为 1024 行 (可用 10 位表示)。主存地址的最低 4 位为 Cache 的行内地址, 中间 10 位为 Cache 行号。如果内存地址为 1234E8F8H, 那么最后 4 位就是 1000 (对应十六进制数的最后一位), 而中间 10 位, 则应从 E8F (111010001111) 中获取, 得到 1010001111。

② 全相联映射: 将主存中一个块的地址与块的内容一起存于 Cache 的行中, 任一主存

块能映射到 Cache 中任意行（主存块的容量等于 Cache 行容量）。速度更快，但控制复杂。

③ 组相联映射：是前两种方式的折中方案。它将 Cache 中的块再分成组，然后通过直接映射方式决定组号，再通过全相联映射的方式决定 Cache 中的块号。

注意：在 Cache 映射中，主存和 Cache 存储器均分成容量相同的块。

例如，容量为 64 块的 Cache 采用组相联方式映射，字块大小为 128 个字，每 4 块为一组。若主存容量为 4096 块，且以字编址，那么主存地址应该为多少位？主存区号为多少位？这样的题目，首先根据主存块与 Cache 块的容量须一致，得出内存块也是 128 个字，因此共有 128×4096 个字，即 2^{19} ($2^7 \times 2^{12}$) 个字，因此需 19 位主存地址；而内存需要分为 $4096/64$ 块，即 64 块，因此主存区号需 6 位。

（3）Cache 淘汰算法

当 Cache 数据已满，并且出现未命中情况时，就要淘汰一些老的数据，更新一些新的数据。选择淘汰什么数据的方法就是淘汰算法。常见的方法有三种：随机淘汰、先进先出（FIFO）淘汰（即淘汰最早调入 Cache 的数据）、最近最少使用（LRU）淘汰法。其中平均命中率最高的是 LRU 算法。

（4）Cache 存储器的写操作

在使用 Cache 时，需要保证其数据与主存一致，因此在写 Cache 时就需要考虑与主存间的同步问题，通常使用以下三种方法：写直达（写 Cache 时，同时写主存）、写回（写 Cache 时不马上写主存，而是等其淘汰时回写）、标记法。

4. 寻址方式

在计算机中，CPU 都会定义出自己特定的指令系统，不过都遵循着统一的标准格式。指令的基本格式是由操作码和地址码两部分组成的。操作码指出该指令要完成什么操作，地址码则提供原始的数据。指令系统中定义操作码的方式可以分为规整型（定长编码）和非规整型（变长编码）两种，如表 1-5 所示。

表 1-5 指令系统中的操作码

编 码 方 式	含 义	平 均 码 长
定长编码	采用相等码长，每个操作码的长度相等	码长大于等于 $\log_2 X$ ，其中 X 为操作码数。例如，14 个操作码，就应该是 4 位。因为 $2^3=8$ ，不够； $2^4=16$ ，多 2 个
变长编码	根据使用频度选择不同长度的编码	将长度分为几类，然后再对每类进行编码。 平均码长：将每个码长乘以频度，再累加其和

在指令系统中用来确定如何提供操作数或提供操作数地址的方式称为寻址方式（编址方式）。操作数可以存放在 CPU 中的寄存器（用寄存器名操作）、主存储器（指出存储单元地址）、堆栈（先进后出的存储机制，用栈顶指针 SP 来标出其当前位置）、外存储器或外围设备中。不过在运算时，数据均在主存储器中，操作数可以采用以下几种寻址方式。

- （1）立即寻址：直接给出操作数，而非地址。
- （2）直接寻址：直接给出操作数地址或所在寄存器号（寄存器寻址）。
- （3）间接寻址：给出的是指向操作数地址的地址，称为间接寻址。
- （4）变址寻址：给出的地址需与特定的地址值累加从而得出操作数地址，称为变址寻址。

通过采用不同的寻址方式,能够达到缩短指令长度、扩大寻址空间和提高编程灵活性等目的。

例如,某计算机字长为 16 位,运算器为 16 位,有 16 个 16 位通用寄存器,8 种寻址方式,主存容量为 64K 字。指令中地址码由寻址方式字段和寄存器字段组成,采用单字长指令。那么要表示 8 种寻址方式需要 3 位,要表示 16 个通用寄存器则需要 4 位,所以地址码一共需要 7 位;而又采用单字长指令,字长为 16 位,因此,操作码的位数就只有 $16-7=9$ 位。也就是说,可以表示的指令种类是 29 条,即 512 条。因为每个寄存器是 16 位的,所以,可以表示的地址范围是 2^{16} 字,即 64K 字。

1.4.2 一点一练

试题 1

某计算机内存按字节编址,内存地址区域从 44000H 到 6BFFFH,共有 (1) K 字节。若采用 16×4bit 的 SRAM 芯片,构成该内存区域共需 (2) 片。

- (1) A. 128 B. 160 C. 180 D. 220
(2) A. 5 B. 10 C. 20 D. 32

试题 2

如果计算机断电,则 (3) 中的数据会丢失。

- (3) A. ROM B. EPROM C. RAM D. 回收站

试题 3

计算机指令系统中采用不同寻址方式可以提高编程灵活性,立即寻址是指 (4) 。

- (4) A. 操作数包含在指令中 B. 操作数的地址包含在指令中
C. 操作数在地址计数器中 D. 操作数在寄存器中

试题 4

如果主存容量为 16M 字节,且按字节编址,表示该主存地址至少应需要 (5) 位。

- (5) A. 16 B. 20 C. 24 D. 32

试题 5

操作数所处的位置,可以决定指令的寻址方式。操作数包含在指令中,寻址方式为 (6) ;操作数在寄存器中,寻址方式为 (7) ;操作数的地址在寄存器中,寻址方式为 (8) 。

- (6) A. 立即寻址 B. 直接寻址
C. 寄存器寻址 D. 寄存器间接寻址
(7) A. 立即寻址 B. 相对寻址
C. 寄存器寻址 D. 寄存器间接寻址
(8) A. 相对寻址 B. 直接寻址
C. 寄存器寻址 D. 寄存器间接寻址

试题 6

若内存地址区间为 4000H~43FFFH,每个存储单元可存储 16 位二进制数,该内存区域由 4 片存储器芯片构成,则构成该内存所用的存储器芯片的容量是 (9) 。

- (9) A. 512×16bit B. 256×8bit C. 256×16bit D. 1024×8bit

试题 7

计算机内存一般分为静态数据区、代码区、栈区和堆区,若某指令的操作数之一采用立

即数寻址方式，则该操作数位于（10）。

- (10) A. 静态数据区 B. 代码区 C. 栈区 D. 堆区

试题 8

（11）是指按内容访问的存储器。

- (11) A. 虚拟存储器 B. 相联存储器
C. 高速缓冲存储器 D. 随机访问存储器

试题 9

以下关于 Cache 的叙述中，正确的是（12）。

- (12) A. 在容量确定时，替换算法的时间复杂度是影响 Cache 命中率的关键因素
B. Cache 的设计思想是在合理成本下提高命中率
C. Cache 的设计目标是容量尽可能与主存容量相等
D. CPU 中的 Cache 容量应大于 CPU 之外的 Cache 容量

试题 10

下列存储设备中，存取速度最快的是（13）。

- (13) A. 主存 B. 辅存 C. 寄存器 D. 高速缓存

1.4.3 解析与答案

试题 1 分析

(1) 内存区域从 44000H 到 6BFFFH，则其拥有的字节数为：

$$6BFFFH - 44000H + 1 = 6C000H - 44000H = 28000H = 1024 \times 158 = 160KB$$

(2) 采用 16K×4bit 的 SRAM 的芯片，则其需要的芯片数为： $(160K/16K) \times (8/4bit) = 20$ 。

试题 1 答案

- (1) B (2) C

试题 2 分析

内存储器分为 ROM 和 RAM 两种类型。

ROM 是只读存储器，是 Read Only Memory 的缩写。ROM 中的内容在厂家生产时写入，其内容只能读出不能改变，断电后其中的内容不会丢失。EPROM (Erasable Programmable Read Only Memory, EPROM) 是可擦除可编程的只读存储器，即 EPROM 中的内容既可以读出，也可以由用户写入，写入后还可以修改。改写的方法是写入之前先用紫外线照射 15~20 分钟以擦去所有信息，然后再用特殊的电子设备写入信息，因此断电不会导致 EPROM 中的内容丢失。回收站是操作系统在磁盘中设置的一个区域，用于记录被删除的文件，需要时恢复。计算机断电时，磁盘中的数据不会丢失。

RAM 是 Random Access Memory 的缩写，是内存储器的主要组成部分，既能从中读取数据也能存入数据。这类存储器的特点是存储信息的易失性，即一旦去掉存储器的供电电源，则存储器所存信息也随之丢失。

试题 2 答案

- (3) C

试题 3 分析

寻址方式是指如何对指令中的地址字段进行解释，以获得操作数的方法或获得程序转移地址的方法。常见的寻址方式有立即寻址、直接寻址、间接寻址、寄存器寻址、寄存器间接寻址、相对寻址和变址寻址等。在立即寻址方式中，操作数包含在指令中；在直接寻址方式

中，操作数存放在内存单元中，指令中直接给出操作数所在存储单元的地址；在寄存器寻址方式中，操作数存放在某一寄存器中，指令中给出存放操作数的寄存器名；在寄存器间接寻址方式中，指令中给出了操作数地址的地址；在相对寻址方式中，在指令地址码部分给出一个偏移量（可正可负），操作数地址等于本条指令的地址加上该偏移量；在变址寻址方式中，操作数地址等于变址寄存器的内容加偏移量。

试题 3 答案

(4) A

试题 4 分析

本题考查主存的计算。

根据主存容量或是芯片的规格要求地址的位数，或是数据线的数量，这种题型在软考中经常出现，但知道规则很容易解题。求地址线只要把主存的内容写成 2 的 N 次方的形式，这个 N 就是地址的位数，如题目中的 16M 等于 2^{24} ，表示该主存地址至少需要 24 位。其实这种规律也是从实践过程中总结出来的，我们来看几个简单的例子：

- ① 如果地址线有 1 根，则可以表示 2 种地址，即地址 0 和地址 1，刚好满足 $2^1=2$ 。
- ② 如果地址线有 2 根，则可以表示 4 种地址，即地址 00、01、10、11，满足 $2^2=4$ 。
- ③ 如果地址线有 3 根，则可以表示 8 种地址，也满足 $2^3=8$ 。

以此类推，也就把规律总结出来了。

试题 4 答案

(5) C

试题 5 分析

此题考查的是考生对操作数几种基本寻址方式的理解。操作数寻址有以下方式。

① 立即寻址

指令的地址字段指出的不是操作数的地址，而是操作数本身。这种方式的特点是指令执行时间很短，不需要访问内存取数。题目中所说的“操作数包含在指令中的寻址方式”就是立即寻址。

例如，单地址的移位指令格式为

OP (移动)	F	D
---------	---	---

这里 D 不是地址，而是一个操作数。F 为标志位，当 $F=1$ ，操作数进行右移；当 $F=0$ 时，操作数进行左移。

② 寄存器寻址方式和寄存器间接寻址方式

当操作数不放在内存中，而是放在 CPU 的通用寄存器中时，可采用寄存器寻址方式。此时指令中给出的操作数地址不是内存的地址单元号，而是通用寄存器的编号。这也就是题目中所说的“操作数在寄存器中的寻址方式”。

寄存器间接寻址方式与寄存器寻址方式的区别在于指令格式中的寄存器内容不是操作数，而是操作数的地址，该地址指明的操作数在内存中。这也就是题目中所说的“操作数的地址在寄存器中的寻址方式”。

试题 5 答案

(6) A

(7) C

(8) D

试题 6 分析

首先将地址编码转换为十进制数， $4000H=1638410$ ， $43FFH16=740710$ ，然后令两个地

址码相减再加 1，即得到这段地址空间中存储单元的个数。 $17407-16384+1=1024$ ，因此共有 1024 个内存单元。 $1024 \times 16b/4=256 \times 16b$ ，因此芯片的容量为 $256 \times 16b$ 。

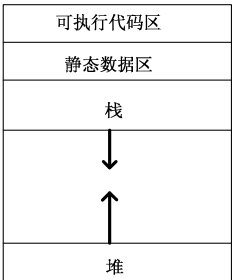


图 1-4 内存空间划分图

试题 6 答案

(9) C

试题 7 分析

本题考查运行过程中计算机内存布局及指令寻址方式。

计算机运行时的内存空间划分情况如图 1-4 所示。

运行时为名字分配存储空间的过程称为绑定。

静态数据区用于存放一对一的绑定且编译时就可确定存储空间

大小的数据，栈用于存放一对多的绑定且与活动同生存期的绑定，堆用于存储由程序语句动态生成和撤销的数据。程序运行时，需要将程序代码（机器指令序列）和代码所操作的数据加载至内存。指令代码加载至代码区，数据则根据绑定关系可能位于静态数据区、栈或堆区。

立即数寻址方式是指指令所需的操作数由指令的地址码部分直接给出，其特点是取指令的同时取出操作数，以提高指令的执行速度。

试题 7 答案

(10) B

试题 8 分析

本题考查计算机系统存储器方面的基础知识。

计算机系统的存储器按所处的位置可分为内存和外存。按构成存储器的材料，可分为磁存储器、半导体存储器和光存储器。按存储器的工作方式可分为读/写存储器和只读存储器。按访问方式可分为按地址访问的存储器和按内容访问的存储器。按寻址方式可分为随机存储器、顺序存储器和直接存储器。

相联存储器是一种按内容访问的存储器。

试题 8 答案

(11) B

试题 9 分析

本题考查高速缓存基础知识。

Cache 是一个高速小容量的临时存储器，可以用高速的静态存储器（SRAM）芯片实现，可以集成到 CPU 芯片内部，或者设置在 CPU 与内存之间，用于存储 CPU 最经常访问的指令或者操作数据。Cache 的出现是基于两种因素：首先是由于 CPU 的速度和性能提高很快而主存速度较低且价格高，其次是程序执行的局部性特点。因此，才将速度比较快而容量有限的 SRAM 构成 Cache，目的在于尽可能发挥 CPU 的高速度。很显然，要尽可能发挥 CPU 的高速度，就必须用硬件实现其全部功能。

试题 9 答案

(12) B

试题 10 分析

计算机的存储器系统由分布在计算机各个不同部件的多种存储设备组成，包括 CPU 内部的寄存器、用于控制单元的控制存储器、内部存储器（由处理器直接存取的存储器，又称为主存储器）、外部存储器（需要通过 I/O 系统与之交换数据，又称为辅助存储器）。它们之间的存取速度情况为：内部存储器快于外部存储器、主存工作在 CPU 和外存之间，速度也

是介于二者之间。而高速缓存是用来缓解主存和 CPU 速度不匹配的问题，速度介于二者之间。所以这几个存储器其存取速度由快至慢排列依次是：CPU 内部的寄存器、高速缓存（Cache）、主存（内存）、辅助存储器（外存）。

试题 10 答案

(13) C

1.5 中断、流水线以及性能评估

该知识点的考查重点把握三个方面的内容：DMA 工作方式、流水线执行时间的计算、可靠性计算。

1.5.1 考点精讲

涉及中断这一模块的考题相对较少，是整个章节中相对次要的部分。流水线与实际工作中的流水作业其实是相似的，考生可以结合这个日常生活中的场景进行理解。在性能评估方面，主要考查系统可靠性、指令周期。

1. 中断方式

在计算机中，I/O 系统可以有 3 种不同的工作方式，分别是程序控制方式、程序中断方式和 DMA 工作方式。

(1) 程序控制方式

在程序控制方式模式下，输入/输出完全由 CPU 控制，在整个 I/O 过程中 CPU 必须等待其完成，限制了 CPU 的高速能力。不过这种方式是由程序主动查询外设，完成主机与外设间的数据传送，方法简单，硬件开销小。

在这种方式下，I/O 设备有两种编码方式。

① 存储器映射：即 I/O 设备和主存储器统一编址，使用相同的机器指令来访问内存和外设，这种方式下，CPU 是采用地址的不同来区分访问的是外设还是存储器的。

② 独立编址：I/O 设备和主存储器的地址空间相互独立，CPU 使用专门的 I/O 指令来访问外设。

程序查询时，CPU 既可以进行串行点名，也可以进行并行查询。

① 串行点名：CPU 依次对所有的外设进行查询，不过每次只查询一台。

② 并行查询：将各个外设的状态位集中起来，由 CPU 通过一个专用的端口来读取，每次可以同时查询多个外设的状态。

(2) 程序中断方式

在 I/O 控制中引入中断，是为了解决“程序控制输入/输出”方法中 CPU 低效等待的缺陷。采用该机制，CPU 将无须定期查询 I/O 系统的状态，节约时间。当 I/O 系统完成后，则以中断信号通知 CPU，之后 CPU 保存正在执行程序现场（包括程序计数器 PC，记住执行到哪个指令），然后转入 I/O 中断服务程序完成数据交换。而收到中断请求后，停止正在执行的代码，保存现场的时间称为中断响应时间，这个时间应该尽可能短。

在系统中有多个中断源时，常见的处理方法如下。

① 多中断信号线法：就是给每个中断源“拉一根电话线”，做到专线专用。

② 中断软件查询法：CPU 收到中断后转到中断服务程序，由该程序来确认中断源。

③ 菊花链法：硬件查询法，所有的 I/O 模块共享一条共同的中断请求线。

④ 总线仲裁法：一个 I/O 设备在发出中断请求前，必须先获得总线控制权。由总线仲裁机制来决定谁有权发出中断信号。

⑤ 中断向量表法：中断向量表用来保存各个中断源的中断服务程序的入口地址，当外设发出中断后，由中断控制器确定其中断号。

(3) DMA 工作方式

中断法虽然比程序控制法更加有效，但由于都是由软件来完成工作的，因此难以满足高速传输的要求。而 DMA 工作方式则使用 DMA 控制器（DMAC）来控制和管理数据传输。DMAC 与 CPU 共享系统总线，并且具有可以独立访问存储器的能力。

在进行 DMA 时，CPU 放弃对系统总线的控制，改由 DMAC 控制总线；由 DMAC 提供存储器地址及必需的读/写控制信号，实现外设与存储器的数据交换。

① 向 CPU 申请 DMA 传送。

② 获得 CPU 允许后，DMA 控制器接管系统总线的控制权。

③ 在 DMA 控制器的控制下，在存储器和外设之间进行数据传送，在传送过程中无须 CPU 参与，开始时需要提供传送数据的长度和起始地址。

④ 传送结束后，向 CPU 返回 DMA 操作完成信号。

DMAC 获取系统总线的控制权可以采用暂停方式（CPU 交出控制权到 DMA 操作结束）、周期窃取方式（CPU 空闲时暂时放弃总线，插入一个 DMA 周期）、共享方式（CPU 不使用系统总线时，由 DMAC 来进行 DMA 传输）。

2. 流水线

流水线技术是通过并行硬件来提高系统性能的常用方法，它其实是一种任务分解的技术，把一件任务分解为若干顺序执行的子任务，不同的子任务由不同的执行机构来负责执行，而这些执行机构可以同时并行工作。

关于流水线这个知识点，主要考查流水线的概念、性能，以及有关参数的计算。

(1) 流水线执行计算

假定有某种类型的任务，共可分成 n 个子任务，每个子任务需要时间 t ，则完成该任务所需的时间即为 $nx \cdot t$ 。若以传统的方式，则完成 k 个任务所需的时间是 $k \cdot n \cdot t$ ；而使用流水线技术执行，则花费的时间是 $(n+k-1) \times t$ 。也就是说，除了第一个任务需要完整的时间外，其他都通过并行，节省了大量的时间，只需一个子任务的单位时间就够了。

另外要注意的是，如果每个子任务所需的时间不同，则其速度取决于其执行顺序中最慢的那个（也就是流水线周期值等于最慢的那个指令周期），要根据实际情况进行调整。

例如，若指令流水线把一条指令分为取指、分析和执行三部分，且三部分的时间分别是取指 2ns，分析 2ns，执行 1ns。那么，最长的是 2ns，因此 100 条指令全部执行完毕需要的时间就是： $(2+2+1) + (100-1) \times 2 = 203\text{ns}$ 。

另外，还应该掌握两个关键的术语：流水线的吞吐率和加速比。流水线的吞吐率（Through Put Rate, TP）是指在单位时间内流水线所完成的任务数量或输出的结果数量。完成同样一批任务，不使用流水线所用的时间与使用流水线所用的时间之比称为流水线的加速比（Speed-Up Ratio）。

例如，在上述例子中，203ns 的时间内完成了 100 条指令，则从指令的角度来看，该流水线的吞吐率为： $(100 \times 10^9) / 203 = 4.93 \times 10^8 / \text{s}$ （ $1\text{s} = 10^9\text{ns}$ ），加速比为 $500 / 203 = 2.46$ （如果不采

用流水线，则执行 100 条指令需要 500ns)。

(2) 影响流水线的主要因素

流水线的关键在于“重叠执行”，因此如果这个条件不能够满足，流水线就会被破坏。这种破坏主要来自 3 种情况。

① 转移指令。因为前面的转移指令还没有完成，流水线无法确定下一条指令的地址，因此也就无法向流水线中添加这条指令。从这里的分析可以看出，无条件跳转指令是不会影响流水线的。

② 共享资源访问的冲突。也就是后一条指令需要使用的数据，与前一条指令发生的冲突，或者相邻的指令使用了相同的寄存器，这也会使流水线失败。为了避免冲突，就需要把相互有关的指令进行阻塞，这样就会引起流水线效率的下降。一般地，指令流水线级数越多，越容易导致数据相关，阻塞流水线。

当然，也可以在编译系统上进行设置，当发现相邻的语句存在资源共享冲突的时候，在两者之间插入其他语句，将两条指令进入流水线的时间拉开，以避免错误。

③ 响应中断。当有中断请求时，流水线也会停止。流水线响应中断有两种方式，一种是立即停止现有的流水线，称为精确断点法，这种方法能够立即响应中断，缩短了中断响应时间，但是增加了中央处理器的硬件复杂度。

还有一种是在中断时，在流水线内的指令继续执行，停止流水线的入口，当所有流水线内的指令全部执行后，再执行中断处理程序。这种方式中断响应时间较长，这种方式称为不精确断点法，优点是实现控制简单。

3. 性能评估

我们通常使用 RAS 来衡量一个计算机系统，即可靠性 (R)、可用性 (A) 和可维护性 (S)。

(1) 基本定义

① 系统的可靠性：是指从系统开始运行 ($t=0$) 到某时刻 t 中能够正常运行的概率，通常用 $R(t)$ 表示。

② 失效率：是指单位时间内失效的元件数与元件总数的比例，通常用 λ 表示。当 λ 为常数时，可靠性与失效率的关系为： $R(t)=e^{-\lambda t}$ 。

③ 平均无故障时间 (MTBF)：是指两次故障间系统能够正常工作的时间平均值。 $MTBF = 1/\lambda$ 。

④ 平均修复时间 (MTRF)：是指从故障发生到机器修复所需的平均时间。它用于表示计算机的可维修性。

⑤ 可用性 (A)：是指计算机的使用效率，它以系统在执行任务的任意时刻能够正常工作的概率来表示。 $A=MTBF/(MTBF+MTRF)$ 。

(2) 系统可靠性模型

① 串联系统：假设一个系统由 n 个子系统组成，当且仅当所有的子系统都能正常工作时，系统才能正常工作，这种系统称为串联系统，如图 1-5 所示。

设系统各个子系统的可靠性分别用 R_1, R_2, \dots, R_n 表示，则系统的可靠性为： $R=R_1 \times R_2 \times \dots \times R_n$ 。

如果系统的各个子系统的失效率分别用 $\lambda_1, \lambda_2, \dots, \lambda_n$ 来表示，则系统的失效率为：

$$\lambda = \lambda_1 + \lambda_2 + \cdots + \lambda_n。$$

② 并联系统：假设一个系统由 n 个子系统组成，只要有一个子系统能够正常工作，系统就能正常工作，如图 1-6 所示。

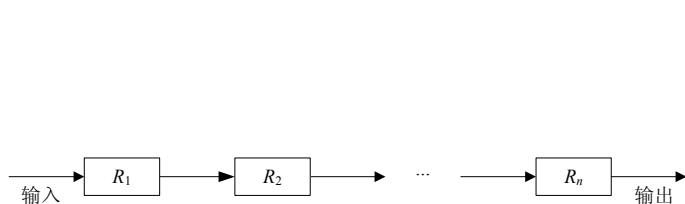


图 1-5 串联系统

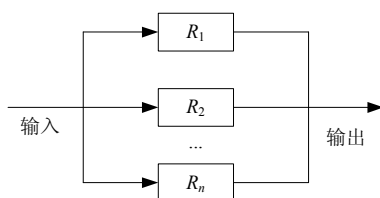


图 1-6 并联系统

设系统各个子系统的可靠性分别用 R_1, R_2, \cdots, R_n 表示，则系统的可靠性为： $R = 1 - (1 - R_1) \times (1 - R_2) \times \cdots \times (1 - R_n)。$

假如所有的子系统的失效率均为 λ ，则系统的失效率为 μ ：

$$\mu = \frac{1}{\frac{1}{\lambda} \sum_{j=1}^n \frac{1}{j}}$$

在并联系统中只有一个子系统是真正需要的，其余 $n-1$ 个子系统称为冗余子系统，随着冗余子系统数量的增加，系统的平均无故障时间也增加了。

③ 模冗余系统： m 模冗余系统由 m 个 ($m=2n+1$ 为奇数) 相同的子系统和一个表决器组成，经过表决器表决后， m 个子系统中占多数相同结果的输出作为系统的输出，如图 1-7 所示。

在 m 个子系统中，只有 $n+1$ 个或 $n+1$ 个以上子系统能正常工作，系统就能正常工作，输出正确结果。假设表决器是完全可靠的，每个子系统的可靠性为 R_0 ，则 m 模冗余系统的可靠性为： $R = \sum_{i=n+1}^m C_m^i \times R_0^i (1 - R_0)^{m-i}$ ，其中 C_m^j 为从 m 个元素中取 j 个元素的组合数。

例如，某高可靠性计算机系统由如图 1-8 所示的冗余部件构成。

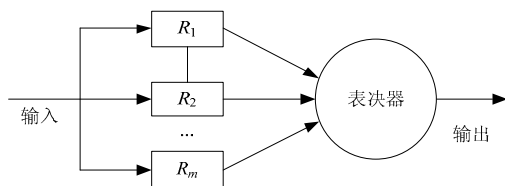


图 1-7 冗余系统

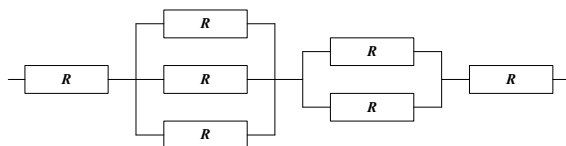


图 1-8 某计算机系统

显然，该系统为一个串、并联综合系统，我们可以先计算出中间 2 个并联系统的可靠度，根据并联公式 $R = 1 - (1 - R_1) \times (1 - R_2) \times \cdots \times (1 - R_n)$ ，可得到 3 个部件并联的可靠度为 $1 - (1 - R)^3$ ，2 个部件并联的可靠度为 $1 - (1 - R)^2$ 。

然后，再根据串联公式 $R = R_1 \times R_2 \times \cdots \times R_n$ ，可得到整个系统的可靠度为 $R \times (1 - (1 - R)^3) \times (1 - (1 - R)^2) \times R。$

1.5.2 一点一练

试题 1

某种部件使用在 10000 台计算机中，运行工作 1000 小时后，其中 20 台计算机的这种部

件失效, 则该部件千小时可靠度 R 为 (1)。

- (1) A. 0.990 B. 0.992 C. 0.996 D. 0.998

试题 2

两个部件的可靠度 R 均为 0.8, 由这两个部件串联构成的系统的可靠度为 (2); 由这两个部件并联构成的系统的可靠度为 (3)。

- (2) A. 0.8 B. 0.64 C. 0.90 D. 0.96
(3) A. 0.8 B. 0.64 C. 0.90 D. 0.96

试题 3

某计算机系统的可靠性如图 1-9 所示的双重串并联结构, 若所构成系统的每个部件的可靠度为 0.9, 即 $R=0.9$, 则该系统的可靠度为 (4)。

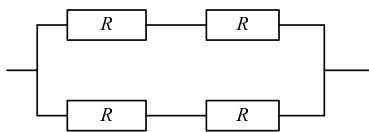


图 1-9 可靠性结构框图

- (4) A. 0.9997 B. 0.9276 C. 0.9639 D. 0.6561

试题 4

若每一条指令都可以分解为取指、分析和执行三步。已知取指时间 $t_{\text{取指}}=5\Delta t$, 分析时间 $t_{\text{分析}}=2\Delta t$, 执行时间 $t_{\text{执行}}=5\Delta t$ 。如果按顺序方式从头到尾执行完 500 条指令需 (5) 位 Δt 。如果按照[执行]_k、[分析]_{k+1}、[取指]_{k+2} 重叠的流水线方式执行指令, 从头到尾执行完 500 条指令需要 (6) 位 Δt 。

- (5) A. 5590 B. 5595 C. 6000 D. 6007
(6) A. 2492 B. 2500 C. 2510 D. 2515

试题 5

某系统的可靠性结构框图如图 1-10 所示。该系统由 4 个部件组成, 其中 2、3 两个部件并联冗余, 再与 1、4 部件串联构成。假设部件 1、2、3 的可靠度分别为 0.90、0.70、0.70。若要求该系统的可靠度不低于 0.75, 则进行系统设计时, 分配给部件 4 的可靠度至少应为 (7)。

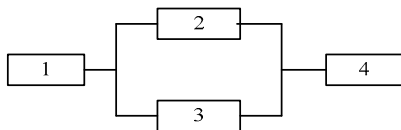


图 1-10 可靠性结构框图

- (7) A. $0.75/[0.9 \times (1-0.7)^2]$ B. $0.75/[0.9 \times (1-0.7 \times 0.7)^2]$
C. $0.75/[0.9 \times (1-(1-0.7)^2)]$ D. $0.75/[0.9 \times (0.7+0.7)]$

试题 6

若某计算机系统由两个部件串联构成, 其中一个部件的失效率为 7×10^{-6} /小时。若不考虑其他因素的影响, 并要求计算机系统的平均故障间隔时间为 10^5 小时, 则另一个部件的失效率应为 (8)/小时。

- (8) A. 2×10^{-5} B. 3×10^{-5} C. 4×10^{-6} D. 3×10^{-6}

试题 7

若每一条指令都可以分解为取指、分析和执行三步。已知取指时间 $t_{\text{取指}}=4\Delta t$ ，分析时间 $t_{\text{分析}}=3\Delta t$ ，执行时间 $t_{\text{执行}}=5\Delta t$ 。如果按串行方式执行完 100 条指令需要 (9) Δt 。如果按照流水方式执行，执行完 100 条指令需要 (10) Δt 。

- (9) A. 1190 B. 1195 C. 1200 D. 1205
(10) A. 504 B. 507 C. 508 D. 510

试题 8

关于在 I/O 设备与主机间交换数据的叙述，(11) 是错误的。

- (11) A. 中断方式下，CPU 需要执行程序来实现数据传送任务
B. 中断方式和 DMA 方式下，CPU 与 I/O 设备都可同步工作
C. 中断方式和 DMA 方式中，快速 I/O 设备更适合采用中断方式传递数据
D. 若同时接到 DMA 请求和中断请求，CPU 优先响应 DMA 请求

试题 9

某指令流水线由 5 段组成，第 1、3、5 段所需时间为 Δt ，第 2、4 段所需时间分别为 $3\Delta t$ 、 $2\Delta t$ ，如图 1-11 所示，那么连续输入 n 条指令时的吞吐率（单位时间内执行的指令个数）TP 为 (12)。

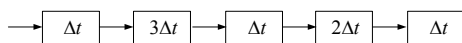


图 1-11 指令流水线图

- (12) A. $n/[5 \times (3+2)\Delta t]$ B. $n/[(3+3+2)\Delta t + 3(n-1)\Delta t]$
C. $n/[(3+2)\Delta t + 3(n-3)\Delta t]$ D. $n/[(3+2)\Delta t + 5 \times 3\Delta t]$

试题 10

在输入/输出控制方法中，采用 (13) 可以使得设备与主存间的数据块传送无须 CPU 干预。

- (13) A. 程序控制输入/输出 B. 中断
C. DMA D. 总线控制

1.5.3 解析与答案

试题 1 分析

根据可靠度的定义，计算如下：

$R=(10000-20)/10000=0.998$ ，即该部件的千小时可靠度为 0.998。

试题 1 答案

(1) D

试题 2 分析

串联的可靠度 $=R \times R=0.64$ 。

并联的可靠度 $=1-(1-R) \times (1-R)=1-0.04=0.96$ 。

系统可靠度计算如下。

并联系统： $1-(1-R_1) \times (1-R_2)$ 。

串联系统： $R_1 \times R_2$ (R 为单个系统的可靠度)。

试题 2 答案

(2) B (3) D

试题 3 分析

题中的结构式一典型的双重并联系统的结构，而且构成系统的四个部件的可靠度均为 0.9。则系统的可靠度可直接由公式求得： $R=2R^2-R^4=0.9639$ 。

试题 3 答案

(4) C

试题 4 分析

顺序执行时，每条指令都需三步才能执行完，没有重叠。总的执行时间为：

$$(5+2+5)\Delta t \times 500 = 6000\Delta t$$

在流水线执行时，所用的时间为：

$$t_{\text{取指}} + \max(t_{\text{分析}}, t_{\text{取指}}) + 498 \times \max(t_{\text{取指}}, t_{\text{分析}}, t_{\text{执行}}) + \max(t_{\text{分析}}, t_{\text{执行}}) + t_{\text{执行}} = \\ 5\Delta t + 5\Delta t + 249\Delta t + 5\Delta t + 5\Delta t = 2510\Delta t$$

重叠执行时间关系如图 1-12 所示。



图 1-12 流水线重叠执行时间关系图

试题 4 答案

(5) C

(6) C

试题 5 分析

本题考查的是计算机系统硬件方面的基础知识。从可靠性设计角度分析，该试题给出的是一种串并混合系统。首先考虑部件 2 和部件 3 是并联冗余结构，它们的可靠度都为 0.70，两者并联冗余的可靠度为 $1-(1-0.70)^2=0.91$ 。在此基础上，系统可以看作可靠度为 0.90 的部件 1、可靠度为 0.91 冗余部件和部件 4 串联构成，串联系统的可靠度为各部件可靠度之积，要求构成的系统的可靠度不低于 0.75，若设部件 4 的可靠度为 R_4 。则： $0.9 \times (1-(1-0.70)^2) \times R_4 = 0.75$ ，从而可以由下式求出部件 4 的可靠度为：

$$R_4 = 0.75 / [0.9 \times (1-(1-0.70)^2)]$$

试题 5 答案

(7) C

试题 6 分析

根据题意，该计算机系统的总失效率为系统平均故障间隔时间的倒数，即 10^{-5} /小时。而计算机系统的总失效率又是各部件失效率的和。因此，另一个部件的效率最大为 $10^{-5} - 7 \times 10^{-6} = 3 \times 10^{-6}$ ，才能保证计算机系统的平均故障间隔时间为 10^5 小时。

试题 6 答案

(8) D

试题 7 分析

顺序执行时，每条指令都需三步才能执行完，设有重叠。总的执行时间为：

$$(4+3+5)\Delta t \times 100 = 1200\Delta t$$

流水线计算公式是：第一条指令顺序执行时间+（指令条数-1）×流水线周期。

对于此题而言，关键在于取指时间为 $4\Delta t$ ，分析时间为 $3\Delta t$ ，而流水线周期都是 5，而实际完成取指只需要 $4\Delta t$ ，分析只需要 $3\Delta t$ 时间，所以采用流水线的耗时为：

$$(4+3+5)+(100-1)\times 5=507\Delta t$$

试题 7 答案

(9) C

(10) B

试题 8 分析

本题考查 I/O 设备与主机间交换数据的方式和特点。

I/O 设备与主机间进行数据输入/输出主要有直接程序控制方式、中断方式、DMA 方式和通道控制方式。

直接程序控制方式的主要特点是：CPU 直接通过 I/O 指令对 I/O 接口进行访问操作，主机与外设之间交换信息的每个步骤均在程序中表示出来，整个输入/输出过程是由 CPU 执行程序来完成的。

中断方式的特点是：当接口准备好接收数据或向 CPU 传送数据时，就发出中断信号通知 CPU。对中断信号进行确认后，CPU 保存正在执行的程序的现场，转而执行提前设置好的 v_0 中断服务程序，完成一次数据传送的处理。这样，CPU 就不需要主动查询外设的状态，在等待数据期间可以执行其他程序，从而提高了 CPU 的利用率。采用中断方式管理 I/O 设备，CPU 和外设可以并行地工作。

虽然中断方式可以提高 CPU 的利用率，能处理随机事件和实时任务，但一次中断处理过程需要经历保存现场、中断处理和恢复现场等阶段，需要执行若干条指令才能处理一次中断事件，因此这种方式无法满足高速的批量数据传送要求。

直接内存存取（Direct Memory Access, DMA）方式的基本思想是：通过硬件控制实现主存与 I/O 设备间的直接数据传送，数据的传送过程由 DMA 控制器（DMAC）进行控制，不需要 CPU 的干预。在 DMA 方式下，需要 CPU 启动传送过程，即向设备发出“传送一块数据”的命令。在传送过程结束时，DMAC 通过中断方式通知 CPU 进行一些后续处理工作。

DMA 方式简化了 CPU 对数据传送的控制，提高了主机与外设并行工作的程度，实现了快速外设和主存之间成批的数据传送，使系统的效率明显提高。

通道是一种专用控制器，它通过执行通道程序进行 I/O 操作的管理，为主机与 I/O 设备提供一种数据传输通道。用通道指令编制的程序存放在存储器中，当需要进行 I/O 操作时，CPU 只要按约定格式准备好命令和数据，然后启动通道即可；通道则执行相应的通道程序，完成所要求的操作。用通道程序也可完成较复杂的 I/O 管理和预处理，从而在很大程度上将主机从繁重的 I/O 管理工作中解脱出来，提高了系统的效率。

试题 8 答案

(11) C

试题 9 分析

本题考查计算机系统流水线方面的基础知识。

吞吐率和建立时间是使用流水线技术的两个重要指标。吞吐率是指单位时间里流水线处理机流出的结果数。对指令而言，就是单位时间里执行的指令数。流水线开始工作，须经过一定时间才能达到最大吞吐率，这就是建立时间。若 m 个子过程所用时间一样，均为 Δt_0 ，则建立时间 $T_0 = m\Delta t_0$ 。

本题目中，连续输入 n 条指令时，第 1 条指令需要的时间 $(1+3+1+2+1)\Delta t$ ，之后，每隔 $3\Delta t$ 便完成一条指令，即流水线一旦建立好，其吞吐率为最长子过程所需时间的倒数。综合

n 条指令的时间为 $(1+3+1+2+1)\Delta t+(n-1)\times 3\Delta t$, 因此吞吐率为:

$$\frac{n}{(3+3+2)\Delta t+3(n-1)\Delta t}$$

试题 9 答案

(12) B

试题 10 分析

本题考查 CPU 中相关寄存器的基础知识。

计算机中主机与外设间进行数据传输的输入/输出控制方法有程序控制方式、中断方式、DMA 等。

在程序控制方式下, 由 CPU 执行程序控制数据的输入/输出过程。

在中断方式下, 外设准备好输入数据或接收数据时向 CPU 发出中断请求信号, CPU 若决定响应该请求, 则暂停正在执行的任务, 转而执行中断服务程序进行数据的输入/输出处理, 之后再回去执行原来被中断的任务。

在 DMA 方式下, CPU 只需向 DMA 控制器下达指令, 让 DMA 控制器来处理数据的传送, 数据传送完毕再把信息反馈给 CPU, 这样就很大程度上减轻了 CPU 的负担, 可以大大节省系统资源。

试题 10 答案

(13) C

1.6 考前冲刺

试题 1

位于 CPU 与主存之间的高速缓冲存储器 Cache 用于存放部分主存数据的副本, 主存地址与 Cache 地址之间的转换工作由__(1)__完成。

(1) A. 硬件 B. 软件 C. 用户 D. 程序员

试题 2

内存单元按字节编址, 地址 0000A000H~0000BFFFH 共有__(2)__个存储单元。

(2) A. 8192K B. 1024K C. 13K D. 8K

试题 3

相联存储器按__(3)__访问。

(3) A. 地址 B. 先入后出的方式
C. 内容 D. 先入先出的方式

试题 4

若 CPU 要执行的指令为: MOV R1,#45 (即将数值 45 传送到寄存器 R1 中), 则该指令中采用的寻址方式为__(4)__。

(4) A. 直接寻址和立即寻址 B. 寄存器寻址和立即寻址
C. 相对寻址和直接寻址 D. 寄存器间接寻址和直接寻址

试题 5

若某计算机系统的 I/O 接口与主存采用统一编址, 则输入/输出操作是通过__(5)__指令来完成的。

(5) A. 控制 B. 中断 C. 输入/输出 D. 访存

试题 6

在程序的执行过程中, Cache 与主存的地址映像由____(6)____。

- (6) A. 专门的硬件自动完成 B. 程序员进行调度
C. 操作系统进行管理 D. 程序员和操作系统共同协调完成

试题 7

总线复用方式可以____(7)____。

- (7) A. 提高总线的传输带宽 B. 增强总线的功能
C. 减少总线中信号线的数量 D. 提高 CPU 利用率

试题 8

指令系统中采用不同寻址方式的目的是____(8)____。

- (8) A. 提高从内存获取数据的速度 B. 提高从外存获取数据的速度
C. 降低操作码的译码难度 D. 扩大寻址空间并提高编程灵活性

试题 9

某计算机系统由图 1-13 所示的部件构成, 假定每个部件的千小时可靠度都为 R , 则该系统的千小时可靠度为____(9)____。

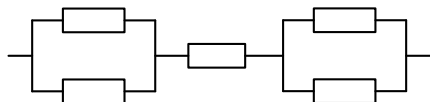


图 1-13 可靠性结构框图

- (9) A. $R+2R/4$ B. $R+R^2/4$ C. $R(1-(1-R)^2)$ D. $R(1-(1-R)^2)^2$

试题 10

若某计算机采用 8 位整数补码表示数据, 则运算____(10)____将产生溢出。

- (10) A. $-127+1$ B. $-127-1$ C. $127+1$ D. $127-1$

试题 11

编写汇编语言程序时, 下列寄存器中程序员可访问的是____(11)____。

- (11) A. 程序计数器 (PC) B. 指令寄存器 (IR)
C. 存储器数据寄存器 (MDR) D. 存储器地址寄存器 (MAR)

试题 12

若某整数的 16 位补码为 FFFF_{H} (H 表示十六进制), 则该数的十进制值为____(12)____。

- (12) A. 0 B. -1 C. $2^{16}-1$ D. $-2^{16}+1$

试题 13

地址码长度为二进制 14 位时, 其寻址范围是____(13)____。

- (13) A. 2KB B. 4KB C. 14KB D. 16KB

试题 14

现有一个 4 级流水线, 分别完成存数、取指、移位、取数 4 种操作。若完成上述操作的时间依次为 4ns 、 5ns 、 6ns 、 7ns , 则流水线的操作周期应该设计为____(14)____ ns 。

- (14) A. 4 B. 5 C. 6 D. 7

试题 15

机器字长 32 位, 其存储容量为 4MB, 若按字编址, 它的寻址范围是____(15)____。

- (15) A. 0~1MW-1 B. 0~1MB-1 C. 0~4MW-1 D. 0~4MB-1

试题 16

若某计算机系统由两个部件串联构成, 其中一个部件的失效率为 7×10^{-6} /小时。若不考虑其他因素的影响, 并要求计算机系统的平均故障间隔时间为 10^5 小时, 则另一个部件的失效率应为 (16) /小时。

- (16) A. 2×10^{-5} B. 3×10^{-5} C. 4×10^{-6} D. 3×10^{-6}

试题 17

CPU 执行一段程序时, Cache 完成存取的次数为 5000 次, 主存完成存取的次数为 200 次。已知 Cache 的存取周期为 40ns, 主存的存取周期为 160ns。其两级存储器的平均访问时间为 (17) ns。

- (17) A. 41 B. 44 C. 44.8 D. 48

试题 18

用 64K×8 的 RAM 芯片和 32K×16 的 ROM 芯片设计一个 256K×16 的存储器, 地址范围为 00000H~3FFFFH, 其中 ROM 的地址范围为 10000H~1FFFFH, 其余为 RAM 的地址。则地址线为 (18) 根; RAM 需要 (19) 片。

- (18) A. 18 B. 9 C. 16 D. 8

- (19) A. 12 B. 2 C. 9 D. 6

试题 19

设一个系统由三个相同子系统并联构成, 子系统的可靠性为 0.9, 平均无故障时间为 10000 小时, 则系统可靠性为 (20), 平均无故障时间为 (21) 小时。

- (20) A. 0.729 B. 0.9 C. 0.999 D. 0.99

- (21) A. 1.9999 B. 18000 C. 9000 D. 18333

试题 20

允许用户在不切断电源的情况下, 更换存在故障的硬盘、电源或板卡等部件的功能是 (22)。

- (22) A. 热插拔 B. 集群技术 C. 虚拟机 D. RAID

试题 21

某种部件使用在 10000 台计算机中, 运行工作 1000 小时后, 其中 20 台计算机的这种部件失效, 则该部件千小时可靠度 R 为 (23)。

- (23) A. 0.990 B. 0.992 C. 0.996 D. 0.998

试题 22

在某计算机系统中, 若某一功能的处理速度被提高到 10 倍, 而该功能的处理使用时间仅占整个系统运行时间的 50%, 那么可使系统的性能大致提高到 (24) 倍。

- (24) A. 1.51 B. 1.72 C. 1.82 D. 1.91

试题 23

下面关于 RISC 计算机的论述中, 不正确的是 (25)。

- (25) A. RISC 计算机的指令简单, 且长度固定
B. RISC 计算机的大部分指令不访问内存
C. RISC 计算机采用优化的编译程序, 有效地支持高级语言
D. RISC 计算机尽量少用通用寄存器, 把芯片面积留给微程序

试题 24

采用 Cache 技术可以提高计算机性能, ____ (26) ____ 属于 Cache 的特征。

- (26) A. 全部用软件实现
B. 显著提高 CPU 数据输入/输出的速率
C. 可以显著提高计算机的主存容量
D. 对程序员是不透明的

试题 25

虚拟存储器是为了使用户可运行比主存容量大得多的程序, 它要在 ____ (27) ____ 之间进行信息动态调度, 这种调度是由操作系统和硬件两者配合来完成的。

- (27) A. CPU 和 I/O 总线 B. CPU 和主存 C. 主存和辅存 D. BIOS 和主存

试题 26

若采用 8K×16bit 存储芯片构成 2M×16bit 的存储器需要 ____ (28) ____ 片。

- (28) A. 128 B. 256 C. 512 D. 不确定

试题 27

评价 CPU 性能一般有三个重要指标, 其中 ____ (29) ____ 不是重要的指标。

- (29) A. CPU 功率 B. 时钟频率
C. 每条指令所花时钟周期数 D. 指令条数

试题 28

____ (30) ____ 是指一批处理对象采用顺序串行执行方式处理所需时间与采用流水执行方式处理所需时间的比值。

- (30) A. 流水线加速比 B. 流水线吞吐率
C. 流水线效率 D. 流水线加速度

试题 29

计算机内存一般分为静态 (static) 数据区、代码区、栈区 (stack) 和堆区 (heap), 若某指令的操作数之一采用立即寻址方式, 则该操作数位于 ____ (31) ____。

- (31) A. 静态数据区 B. 代码区
C. 栈区 D. 堆区

试题 30

高速缓存与主存间采用全相联地址映射方式, 其容量为 4MB。分为 4 块, 每块为 1MB, 主存容量位 256MB。若主存读/写时间为 30ns, 高速缓存的读/写时间为 3ns, 平均读/写时间为 3.27ns, 则该高速缓存的命中率为 ____ (32) ____%; 若地址变换如表 1-6 所示, 则主存地址为 8888888H 时, 高速缓存地址为 ____ (33) ____ H。

表 1-6 地址变化表

0	38H
1	88H
2	59H
3	67H

- (32) A. 90 B. 95 C. 97 D. 99
(33) A. 488888 B. 388888 C. 288888 D. 188888

1.7 习题解析

试题 1 分析

由于在 CPU 与存储系统之间存在着数据传送带宽的限制,因此在其中设置了 Cache (高速缓冲存储器,简称高速缓存,通常速度比内存快),以提高整体效率。但由于其成本更高,因此 Cache 的容量要比内存小得多。由于 Cache 为高速缓存,存储了频繁访问内存中的数据,因此它与 Cache 单元地址转换的工作需要稳定而且高速的硬件来完成。

试题 1 答案

(1) A

试题 2 分析

主存储器(内存)采用的是随机存取方式,需对每个数据块进行编码,而在主存储器中,数据块是以 word 为单位来标识的,即每个字一个地址,通常采用的是十六进制表示。例如,按字节编址,地址从 0000A000H~0000BFFFH,则表示有(0000BFFFH-0000A000H)+1 字节,即 8KB。

试题 2 答案

(2) D

试题 3 分析

存储器的存取方式如表 1-7 所示:

表 1-7 存储器存取方式表

存取方式	读/写装置	数据块标志	访问特性	代表
顺序存取	共享读/写装置	无	特定线性顺序	磁带
直接存取	共享读/写装置	数据分块,每块一个唯一标志	可直接移到特定数据块	磁盘
随机存取	每个可寻址单元专用读/写装置	每个可寻址单元均有一个唯一地址	随时访问任何一个存储单元	主存储器
相联存取(属随机存取)	每个可寻址单元专用读/写装置	每个可寻址单元均有一个唯一地址	根据内容而非地址来选读/写点	Cache

试题 3 答案

(3) C

试题 4 分析

在计算机中需要编址的设备主要有运算器中的通用寄存器、主存储器和输入/输出设备三种。指令在执行的过程中通常需要操作数,运算结果也要送到数据存储单元中进行保存,寻找操作数及数据存储单元的方法称为寻址方式。常见的寻址方式如下。

① 立即寻址:立即寻址方式通常直接在指令的地址码部分给出操作数。这种方式的优点就是不需要数据存储单元,缺点是立即寻址方式通常仅仅用来指定一些精度要求不高的整型常数,数据的长度不能太长。

② 寄存器寻址:指令在执行过程中所需要的操作数来源于寄存器,运算结果也写回到寄存器中,这种寻址方式在所有的 RISC 计算机及大部分的 CISC 计算机中得到广泛应用。它有寄存器直接寻址与间接寻址之分。其中间接寻址,即在通用寄存器中存放的是操作数在主存储器中的地址。

试题 4 答案

(4) B

试题 5 分析

I/O 接口与主存采用统一编址, 即将 I/O 设备的接口与主存单元一样看待, 每个端口占用一个存储单元的地址, 其实就是将主存的一部分划出来作为 I/O 地址空间。

访存指令是指访问内存的指令, 显然, 这里需要访问内存, 才能找到相应的输入/输出设备, 一次需要使用访存指令。

而控制类指令通常是指程序控制类指令, 用于控制程序流程改变的指令, 包括条件转移指令、无条件转移指令、循环控制指令、程序调用和返回指令、中断指令等。

试题 5 答案

(5) D

试题 6 分析

Cache 与主存的地址映像需要专门的硬件自动完成, 使用硬件来处理具有更高的转换速率。

试题 6 答案

(6) A

试题 7 分析

一个信号线传送不同信号, 例如, 地址总线 and 数据总线共用一组信号线。采用这种方式的目的减少总线数量, 提高总线的利用率。

试题 7 答案

(7) C

试题 8 分析

在指令系统中用来确定如何提供操作数或提供操作数地址的方式称为寻址方式, 通过采用不同的寻址方式, 能够达到缩短指令长度、扩大寻址空间和提高编程灵活性等目的。

试题 8 答案

(8) D

试题 9 分析

串联系统: 假设一个系统由 n 个子系统组成, 当且仅当所有的子系统都有能正常工作时, 系统才能正常工作, 这种系统称为串联系统。设系统各个子系统的可靠性分别用 R_1, R_2, \dots, R_n 表示, 则系统的可靠性为 $R \times R_1 \times R_2 \times \dots \times R_n$ 。

并联系统: 假如一个系统由 n 个子系统组成, 只要有一个子系统能够正常工作, 系统就能正常工作。设系统各个子系统的可靠性分别用 R_1, R_2, \dots, R_n 表示, 则系统的可靠性为 $1 - (1 - R_1) \times (1 - R_2) \times \dots \times (1 - R_n)$ 。

本题为串联系统与并联系统互联计算其可靠性, 首先我们计算第一部分的可靠性, 第一部分为并联系统, 其可靠性为: $1 - (1 - R) \times (1 - R)$, 第二部分的可靠性为 R , 第三部分的可靠性为 $1 - (1 - R) \times (1 - R)$ 。三个部分串联后的可靠性为 $R \times [1 - (1 - R) (1 - R)]^2$ 。

试题 9 答案

(9) D

试题 10 分析

本题考查的是数据运算方面的基础知识。

对于有 n 位的整数补码, 其取值范围是 $-2^{n-1} \sim 2^{n-1} - 1$ 。即对于 8 位的整数补码, 其有效取值范围是 $-2^7 \sim 2^7 - 1$, 也就是 $-128 \sim 127$ 。C 答案中的 $127 + 1$ 显然超过了这个取值范围, 固

然会产生溢出。

试题 10 答案

(10) C

试题 11 分析

本题考查 CPU 中相关寄存器的基础知识。

指令寄存器 (IR) 用于暂存从内存取出的、正在运行的指令, 这是由系统使用的寄存器, 程序员不能访问。

存储器数据寄存器 (MDR) 和存储器地址寄存器 (MAR) 用于对内存单元访问时的数据和地址暂存, 也是由系统使用的, 程序员不能访问。

程序计数器 (PC) 用于存储指令的地址, CPU 根据该寄存器的地址从内存读取待执行的指令, 程序员可以访问该寄存器。

试题 11 答案

(11) A

试题 12 分析

正数的最前面一位是符号位, 0 表示正, 1 表示负。而 FFFF 的符号位是负数。而负数的原码等于负数的补码再次求补。因此去掉符号位, 7FFF 再次求补码, 只要按位取反, 再加 1 即可。因此是 $0000000000000000+1$ 得到 000000000001 , 也就是 -1。

试题 12 答案

(12) B

试题 13 分析

此题型其实是软考中的一种常见题, 只是提问方式稍做了变动, 在考试中一般问容量为多少 KB 的芯片有多少根地址线, 这道题其实就是已知地址线的根数, 要求芯片容量。由于 $2^{14}=16K$, 所以此题应选 D。

试题 13 答案

(13) D

试题 14 分析

由流水线基本特征可知, 其平均时间取决于流水线中最慢的操作, 所以流水线的操作周期应该设计为时间最长的那一步。

试题 14 答案

(14) D

试题 15 分析

题目中机器字长 32 位, 表示一个字 (word) 为 4 字节。存储容量为 4MB, 按字编制也就是按 4 字节 (4B) 为单位来规划每个字的地址。那么总共会有 $4MB/4B=1M$ 个字 (1MW), 那么可寻址的范围从 0 开始, 一直到“1MW-1”, 总共还是 1M 个字。最终答案为 $0\sim 1MW-1$ 。

试题 15 答案

(15) A

试题 16 分析

根据题意, 该计算机系统的总失效率为系统平均故障间隔时间的倒数, 即 $10^{-5}/\text{小时}$ 。而计算机系统的总失效率又是各部件失效率的和。因此, 另一个部件的效率最大为

$10^{-5}/H-7\times 10^{-6}/H=3\times 10^{-6}/H$, 才能保证计算机系统的平均故障间隔时间为 10^5 小时。

试题 16 答案

(16) D

试题 17 分析

两级存储器的平均访问时间= $H\times T1+(1-H)\times T2$

CPU 命中率= $5000/(5000+200)\approx 0.96$

平均访问时间= $0.96\times 40ns+(1-0.96)\times 160ns=44.8ns$

试题 17 答案

(17) C

试题 18 分析

因为总容量为 $256K\times 16=2^{18}\times 16$, 所以地址线、数据线分别为 18 根和 16 根。因为 ROM 的地址范围为 $10000H\sim 1FFFFH$, 所以 ROM 的容量为 $1FFFF-10000=FFFF$, FFFF 转换为十进制, 则为 65535, 即 64K。已知用 $32K\times 16$ 的 ROM 芯片来设计, 因此需要 2 片这样的芯片。

RAM 的容量= $256K-64K=192K$, 用 $64K\times 8$ 的 RAM 芯片来设计, 所以需要 6 片。

试题 18 答案

(18) A

(19) D

试题 19 分析

假设一个系统由 n 个子系统组成, 当且仅当所有的子系统都能正常工作时, 系统才能正常工作, 这种系统称为串联系统, 设系统各个子系统的可靠性分别用 $R_1, R_2, R_3\cdots, R_n$ 表示, 则系统的可靠性: $R=R_1\times R_2\times R_3\times\cdots\times R_n$; 如果系统的各个子系统的失效率分别用 $\lambda_1, \lambda_2, \lambda_3\cdots, \lambda_n$ 来表示, 则系统的失效率: $\lambda=\lambda_1+\lambda_2+\lambda_3+\cdots+\lambda_n$ 。

假设本题的三个子系统是串联的, 则 $n=3, R_1=R_2=R_3=0.9, \lambda_1=\lambda_2=\lambda_3=1/10000=0.0001$, 则系统可靠性为: $R=R_1\times R_2\times R_3=0.9\times 0.9\times 0.9=0.729$ 。

系统失效率为: $\lambda=\lambda_1+\lambda_2+\lambda_3=0.0001+0.0001+0.0001=0.0003$ 。

系统平均故障间隔时间: $MTBF=1/\lambda=1/0.0003=3333$ 。

假如一个系统由 n 个子系统组成, 只要有一个子系统能够正常工作, 系统就能正常工作。设系统各个子系统的可靠性分别用 $R_1, R_2, R_3\cdots, R_n$ 表示, 则系统的可靠性: $R=1-(1-R_1)\times(1-R_2)\times(1-R_3)\times\cdots\times(1-R_n)$ 。如果各个子系统的失效率均为 λ_1 , 则系统的失效率: $\lambda=\lambda_1/(1+1/2+\cdots+1/n)$, 系统平均故障间隔时间为 $MTBF=1/\lambda$ 。

在本题中, $n=3, R_1=R_2=R_3=0.9, \lambda=1/10000=0.0001$ 。

系统可靠性为: $R=1-(1-R_1)\times(1-R_2)\times(1-R_3)=1-(1-0.9)\times(1-0.9)\times(1-0.9)=0.999$ 。

系统失效率为: $\lambda=\lambda_1/(1+1/2+1/3)=0.0001/1.8333=0.0000546$ 。

系统平均无故障间隔时间 $MTBF=1/\lambda=(1+1/2+1/3)/\lambda_1=18333$ 。

试题 19 答案

(20) C

(21) D

试题 20 分析

热插拔即带电插拔, 热插拔功能就是允许用户在不关闭系统, 不切断电源的情况下取出和更换损坏的硬盘、电源或板卡等部件, 从而提高了系统对灾难的及时恢复能力、扩展性和灵活性等。

试题 20 答案

(22) A

试题 21 分析

系统的可靠度是指在某段时间内能正常运行的概率, 1000 小时内这种部件用在 10000 台计算机里, 20 台失效, 表明有 $10000-20=9980$ 台能正常运行, 所以这 1000 小时内的可靠度为 $9980/100000=0.998$ 。

试题 21 答案

(23) D

试题 22 分析

假设该处理原来所需时间为 t , 由于该功能的处理使用时间占整个系统运行时间的 50%, 所以, 其他处理时间也为 t 。该功能的处理速度被提高到 10 倍后, 则其所需时间为 $0.1t$, 因此, 系统的性能大致提高到 $(t+t)/(0.1t+t) = 2t/1.1t = 1.82$ 倍。

试题 22 答案

(24) C

试题 23 分析

RISC 计算机的指令简单, 且长度固定, 没有必要采用微程序设计。RISC 计算机仅用 LOAD/STORE 指令访问内存, 使用了大量的寄存器, 采用优化的编译程序, 能有效地支持高级语言。

试题 23 答案

(25) D

试题 24 分析

高速缓冲存储器 (Cache): 在计算机存储系统的层次结构中, 介于中央处理器和主存储器之间的高速小容量存储器。它和主存储器一起构成一级的存储器。高速缓冲存储器和主存储器之间信息的调度和传送是由硬件自动进行的。

Cache 的容量一般只有主存储器的几百分之一, 但它的存取速度能与中央处理器相匹配。根据程序局部性原理, 正在使用的主存储器某一单元邻近的那些单元将被用到的可能性很大。因而, 当中央处理器存取主存储器某一单元时, 计算机硬件就自动地将包括该单元在内的那一组单元内容调入高速缓冲存储器, 中央处理器即将存取的主存储器单元很可能就在刚刚调入到高速缓冲存储器的那一组单元内。于是, 中央处理器就可以直接对高速缓冲存储器进行存取。在整个处理过程中, 如果中央处理器绝大多数存取主存储器的操作能为存取高速缓冲存储器所代替, 计算机系统处理速度就能显著提高。

显然, Cache 可以显著提高 CPU 数据输入/输出的速率。

试题 24 答案

(26) B

试题 25 分析

虚拟存储的作用: 内存在计算机中的作用很大, 计算机中所有运行的程序都需要经过内存来执行, 如果执行的程序很大或很多, 就会导致内存消耗殆尽。为了解决这个问题, Windows 中运用了虚拟内存技术, 即拿出一部分硬盘空间来充当内存使用, 当内存占用完时, 计算机就会自动调用硬盘来充当内存, 以缓解内存的紧张。

虚拟存储器要在主存（如内存）和辅存（如硬盘）之间进行信息动态调度。

试题 25 答案

(27) C

试题 26 分析

需要 $(2\text{M}/8\text{K}) \times (16\text{bit}/16\text{bit})=256$ 片。

试题 26 答案

(28) B

试题 27 分析

本题考查体系结构中的重要指标，即 CPU 性能指标。CPU 性能指标为时钟频率、每条指令所花的时钟周期数（或者是每条指令平均）、指令条数。

试题 27 答案

(29) A

试题 28 分析

流水线加速比是指一批处理对象采用顺序串行执行方式处理所需时间与采用流水执行方式处理所需时间的比值。

试题 28 答案

(30) A

试题 29 分析

栈区由编译器自动分配释放，保存为运行函数而分配的局部变量、函数参数、返回数据及返回地址等，其操作方式类似数据结构中的栈。

堆区一般由程序员分配释放，否则程序结束时可能由 OS 回收，分配方式类似链表。

静态数据区保存全局变量、静态数据和常量，程序结束后由系统释放。

代码区保存函数体（类成员函数和全局函数）的二进制代码。

立即数即常数，在写程序时定义，实际上是一个值。如 `MOV AX FFH` 中的 `FFH` 就是一个值，一个立即数。这样的数放在程序段，而非数据段中。PC 指针指向这个指令时取到代码同时取到数据。

试题 29 答案

(31) B

试题 30 分析

第（32）空是一道简单的计算题，设高速缓存的命中率为 t ，则：

$$30 \times (1-t) + 3 \times t = 3.27$$

解方程式得到 $t=0.99$ 。所以高速缓存的命中率为 99%。

关于第（33）空，由于高速缓存的容量是 4MB，分为 4 块，每块为 1MB，所以把高速缓存的 22 位长地址划分为两部分，块号是 2 位，而块内地址为 20 位。主存容量为 256MB，所以主存地址长度是 28 位。这样主存的块号为 8 位，块内地址为 20 位。此时我们先将主存地址写成 `88H 88888H`，其中斜体 `88H` 为块号，加粗部分 `88888H` 为块内地址。查表 1-8（题干中已经给出）可以得到高速缓存对应块号为 1H，所以其地址为 `188888H`，因此（33）空答案为 D。

表 1-8 地址变化表

0	38H
1	88H
2	59H
3	67H

试题 30 答案

(32) D

(33) D

对于网络工程师考试而言，操作系统属于要了解的内容，偏重对知识点的一些记忆，出题频度与难度都比较低。

2.1 考点脉络

操作系统是网络工程师考试中的一个基础知识点。在最近几次的考试中出题的频率逐年减少。根据考试大纲，要求考生掌握以下几个方面的内容。

- (1) 存储和进程管理：主要考查虚拟存储器、进程状态和调度。
- (2) 文件管理：主要考查文件的组织和结构。

从历年的考试试题来看，本章的考点在综合知识考试中的平均分数为 2.45 分，约为总分 3.26%。考试试题分数主要集中在进程死锁/PV 操作、进程调度、操作系统文件结构这 3 个知识点上。

2.2 存储和进程管理

在存储和进程管理这个考点中，主要涉及虚存管理和进程管理两个方面的内容。

2.2.1 考点精讲

虚拟内存是计算机系统内存管理的一种技术。它使得应用程序认为它拥有连续的可用的内存（一个连续完整的地址空间），而实际上，它通常是被分隔成多个物理内存碎片，还有部分暂时存储在外部磁盘存储器上，在需要时进行数据交换。进程管理是考试中比较关注的一个知识点，考生必须掌握其相关概念和进程互斥的知识。

1. 虚存管理

程序运行过程中可以随机访问内存中的数据或程序，但需要的程序或数据不在内存时，就将内存中部分内容根据情况写回外存，然后从外存调入所需程序或数据，实现作业内部的局部对换，从而允许程序的地址空间大于实际分配的存储区域。它在内存和外存之间建立了层次关系，使得程序能够像访问主存一样访问外存，主要用于解决计算机主存储器的容量问题。其逻辑容量由主存和外存容量之和以及 CPU 可寻址的范围来决定，其运行速度接近于主存速度，成本也下降了。可见，虚拟存储技术是一种性能非常优越的存储器管理技术，故被广泛地应用于大、中、小型机器和微型机中。

虚存管理主要包含了虚拟存储器分类、局部性原理、虚存的载入、放置、置换策略等内容。

(1) 虚拟存储器分类

虚拟存储器允许用户用比主存容量大得多的地址空间来编程，以运行比主存实际容量大

得多的程序。用户编程所用的地址称为逻辑地址（又称虚地址），而实际的主存地址则称为物理地址（又称实地址）。每次访问内存时都要进行逻辑地址到物理地址的转换。实际上，超过主存实际容量的那些程序和数据是存放在辅助存储器中的，当使用时再由辅存调入。地址变换以及主存和辅存间的信息动态调度是硬件和操作系统两者配合完成的。

虚拟存储器可以分为单一连续分区、固定分区、可变分区、可重定位分区、非请求页式、请求页式、段页式 7 种。

① 单一连续分区。把所有用户区都分配给唯一的用户作业，当作业被调度时，进程全部进入内存，一旦完成，所有主存恢复空闲，因此，它不支持多道程序设计。

② 固定分区。这是支持多道程序设计的最简单的存储管理方法，它把主存划分成若干个固定的和大小不同的分区，每个分区能够装入一个作业，分区的大小是固定的，算法简单，但是容易生成较多的存储器碎片。

③ 可变分区。引入可变分区后虽然主存分配更灵活，也提高了主存利用率，但是由于系统在不断的分配和回收中，必定会出现一些不连续的小的空闲区，尽管这些小的空闲区的总和超过某一个作业要求的空间，但是由于不连续而无法分配，产生了碎片。解决碎片的方法是拼接（或称紧凑），即向一个方向（例如向低地址端）移动已分配的作业，使那些零散的小空闲区在另一方向连成一片。分区的拼接技术，一方面要求能够对作业进行重定位，另一方面系统在拼接时要耗费较多的时间。

④ 可重定位分区。这是克服固定分区碎片问题的一种存储分配方法，它能够把相邻的空闲存储空间合并成一个完整的空区，还能够整理存储器内各个作业的存储位置，以达到消除存储碎片和紧缩存储空间的目的。紧缩工作需要花费大量的时间和系统资源。

⑤ 非请求页式。非请求页式将存储空间和作业的地址空间分成若干个等分部分，在执行时，要求把进程所需要的页面全部调入主存后作业方能运行。因此，当内存可用空间小于作业所需的地址空间时，作业无法运行。它克服了分区存储管理中碎片多和紧缩处理时间长的缺点，支持多道程序设计，但不支持虚拟存储。

⑥ 请求页式。请求页式将存储空间和作业的地址空间分成若干个等分部分，在执行时，当进程需要用到某个页面时将该页面调入主存，把那些暂时无关的页面留在主存外。它支持虚拟存储，克服了分区存储管理中碎片多和紧缩处理时间长的缺点，支持多道程序设计，但是它不能实现对最自然的以段为单位的共享与存储保护（因为程序通常是以段为单位划分的，所以以段为单位最自然）。

⑦ 段页式。这是分段式和分页式结合的存储管理方法，充分利用了分段管理和分页管理的优点。作业按逻辑结构分段，段内分页，内存分块。作业只需部分页装入即可运行，所以支持虚拟存储，可实现动态连接和装配。

现在，最常见的虚存组织有分段技术、分页技术、段页式技术 3 种。我们把这 3 种存储组织总结如表 2-1 所示。

表 2-1 三种虚存组织

项 目	段 式 管 理	页 式 管 理	段页式管理
划分方式	段（不定长） 每个作业一张段表	页（定长） 每个进程一张页表	先将主存分为等长页，每个作业一张段表（通常有一个基号指向它），每段对应一张页表
虚地址	(s,d)，即（段号，段内偏移）	(p,d)，即（页号，页内偏移）	(s,p,d)，即（段号、段内页号、页内偏移）
虚实转换	段表内找出起始地址，然后加上段内偏移	页表内找出起始地址，然后加上页内偏移	先在段表中找到页表的起始地址，然后在页表中找到起始地址，最后加上页内偏移

续表

项 目	段 式 管 理	页 式 管 理	段页式管理
主要优点	简化了任意增长和收缩的数据段管理，利于进程间共享过程和数据	消除了页外碎片	结合了段与页的优点 便于控制存取访问
主要缺点	段外碎片降低了利用率	存在页内碎片	增加复杂度，增加硬件， 存在页内碎片

例如，某页式存储系统的地址变换过程如图 2-1 所示。假定页面的大小为 8K，如图 2-1 中所示的十进制逻辑地址 9612 经过地址变换后，形成的物理地址 a 应为十进制多少呢？

因为 $8K=2^{13}$ ，所以页内地址有 13 位。逻辑地址 9612 转换成二进制，得到 10010110001100，这里的低 13 位为页内偏移量，最高一位则为页号，所以逻辑地址 9612 的页号为 1，根据图 2-1 所示的对照表，即物理块号为 3（二进制形式为 11）。把物理块号和页内偏移地址拼合得到 110010110001100，再转换为十进制，得到 25996。

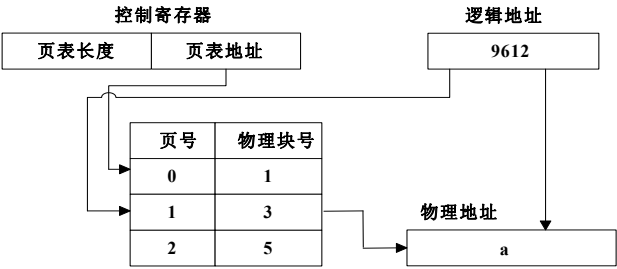


图 2-1 页式存储系统的地址变换过程

在现行的虚存组织方面，最常见的就是段页式管理。在进行虚实地址转换时，可以采用的公式如下：

$$(((x) + s) + p) \times 2^n + d$$

其中 x 为基号， s 为段号， p 为段内页号， d 为页内偏移， n 的值为 d 的总位数， (x) 表示 x 里的内容。

(2) 局部性原理

虚拟存储管理的理论基础是程序的局部性原理。

程序的局部性原理是指程序在执行时呈现出局部性规律，即在一段时间内，程序的执行仅限于程序的某一部分。相应地，执行所访问的存储空间也局限于某个内存区域。局部性又表现为时间局部性和空间局部性。时间局部性是指如果程序中的某条指令一旦执行，则不久以后该指令可能再次执行；如果某数据被访问，则不久以后该数据可能再次被访问。空间局部性是指一旦程序访问了某个存储单元，则不久之后，其附近的存储单元也将被访问。

根据程序的局部性理论，Denning 提出了工作集理论。工作集是指进程运行时被频繁访问的页面集合。显然只要使程序的工作集全部在内存中，就可以大大减少进程的缺页次数；否则会使进程在运行中频繁出现缺页中断，从而出现频繁的页面调入/调出现象，造成系统性能下降，甚至出现“抖动”。

划分工作集可以按定长时间或定长页面两种方法进行。当颠簸现象发生时，说明系统负荷过大，通常采用处理器均衡调度，淘汰低优先级进程。另一种是控制缺页率，当缺页率达到上限时，则增加内存分配量；达到下限时，就减少内存分配量。

(3) 虚存管理

在虚存的管理中涉及载入（调入）、放置（放入分区）和置换（Swapping）等问题。

调入策略，也就是何时将一页或一段从外存中调入主存，通常有两种策略，一种是请求调入法，即需要使用时才调入；另一种是先行调入法，即将预计要使用的页/段先行调入主存。

放置策略，也就是调入后，放在主存的什么位置，这与实存管理基本上是一致的。

置换策略，由于实际主存是小于虚存的，因此可能会发生内存中已满，但需要使用的页不在主存中这一情况（称为缺页中断）。这时就需要进行置换，即将一些主存中的页淘汰到外存，腾出空间给要使用的页，这个过程也称为“Swapping”。如果选择的页面被频繁装入和调出，这种现象称为“抖动”，应减少和避免抖动现象。常见的置换算法如下。

① 最优算法（OPT）：淘汰不用的或最远的将来才用的页。这是一种理想算法，不可能实现，只是用来作为衡量算法效率的参照物。

② 随机算法（RAND）：随机淘汰。这种算法开销小，但性能不稳定。

③ 先进先出算法（FIFO）：选择最早调入（也是驻留时间最长）的页淘汰。

④ 最近最少使用算法（LRU）：选择离当前时刻最近的一段时间内使用得最少的页淘汰。

2. 进程管理

进程管理是考试中比较关注的一个知识点，考生需要掌握其相关概念和进程同步、互斥的知识。

(1) 进程概述和进程状态

进程是一个程序关于某个数据集的一次运行。通俗地说，当打开了两个“QQ”时，其程序是一个，但创建了两个互不相关的进程。进程是运行中的程序，具有动态性和并发性的特点。进程也是系统资源分配、调度、管理的最小单位（现在操作系统中还引入了线程钟，即轻量级进程，它是处理器分配的最小单位）。

一个进程从创建而产生至撤销而消亡的整个生命周期，可以用一组状态加以刻画。为了便于管理进程，把进程划分为3种状态，即进程的运行态、就绪态和阻塞态。

① 运行态：占有处理器时间，代表正在运行。

② 就绪态：具备运行条件，等待系统分配处理器以便运行。

③ 等待态（阻塞态）：不具备运行条件，正在等待某个事件的完成。

一个进程在创建后将处于就绪状态。在执行过程中，每个进程任一时刻都将处于上述3种状态之一。同时，在一个进程执行过程中，它的状态将会发生改变。图2-2表示进程的状态转换。

运行状态的进程将由于出现等待事件而进入等待状态，当等待事件结束之后等待状态的进程将进入就绪状态，而处理器的调度策略又会引起运行状态和就绪状态之间的切换。引起进程状态转换的具体原因如下。

① 运行态→等待态：等待使用资源，如等待外设传输、等待人工干预。

② 等待态→就绪态：资源得到满足，如外设传输结束、人工干预完成。

③ 运行态→就绪态：运行时间片到期，出现有更高优先权的进程。

④ 就绪态→运行态：CPU空闲时选择一个就绪进程。

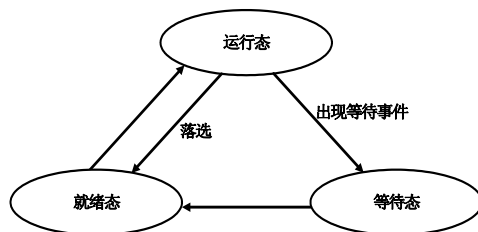


图 2-2 进程三态模型及其状态转换

在操作系统中通常使用进程控制块（PCB）来标记进程，因此从某种意义上来说进程由进程控制块、程序、数据构成。

理解这个基本概念之后更重要的是在此基础上灵活运用。如在一个单 CPU 的计算机系统中采用抢占优先级的进程调度方案，所有任务可以并行使用 I/O 设备。现有 3 个任务 T1、T2、T3，其优先级分别为高、中、低。每个任务都需要先占用 CPU 10ms，然后使用 I/O 设备 13ms，最后占用 CPU 5ms。如果操作系统的开销忽略不计，这 3 个任务从开始到全部结束的总时间是多少 ms？CPU 的空闲时间共有多少 ms？这个问题我们可以通过绘制进程执行状态图来解答，如图 2-3 所示。

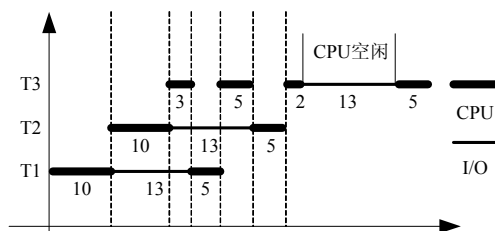


图 2-3 进程执行时空图

我们来对时空图 2-3 作解析，时空图的横轴表示系统运行时间，纵轴分别表示 T1~T3 任务。

① 由于任务 T1~T3 同时启动，且 T1 的优先级别高，所以最先使用 CPU 资源，而其他进程只能处于等待状态。由于 T1 第一占用 CPU 需要 10ms，所以纵轴 T1 刻度上长 10 单位的横线用粗线表示。

② 10ms 后，任务 T1 释放 CPU 资源，这个时候 T1 使用 I/O 设备，时间需要 13ms，所以纵轴 T1 刻度上长 13 单位的横线用细线表示；同时由于这里有 T2、T3 任务还在抢占 CPU 的使用，T2 的优先级别高，所以 T2 使用 CPU 资源而 T3 处于等待状态，由于 T2 第一占用 CPU 需要 10ms，所以纵轴 T2 刻度上长 10 单位的横线用粗线表示。

③ 20ms 后，任务 T2 释放 CPU 资源，这个时候 T2 使用 I/O 设备，时间需要 13ms，所以纵轴 T2 刻度上长 13 单位的横线用细线表示；同时 T3 开始使用 CPU 资源。

④ 23ms 后，T1 执行 I/O 操作完毕，开始再次需要使用 CPU 资源，由于优先级别高，就剥夺了 T3 使用 CPU 的权力，开始执行 CPU。而 T3 又开始等待。

从时空图中可以看出，总时间为 $10+13+5+5+5+2+13+5=58(\text{ms})$ 。在整个时间轴上，CPU 仅在倒数第二段为空闲状态，空闲时间为 13ms。

（2）信号量与 P、V 操作

在操作系统中，进程之间经常会存在互斥（都需要共享独占性资源时）和同步（完成异步的两个进程的协作）两种关系。为了有效地处理这两种情况，W.Dijkstra 在 1965 年提出信

号量和 P、V 操作的概念。

信号量：是一种特殊的变量，表现形式是一个整型 S 和一个队列。

P 操作：也称为 down()、wait()操作，使 $S=S-1$ ，若 $S<0$ ，进程暂停执行，放入信号量的等待队列。

V 操作：也称为 up()、signal()操作，使 $S=S+1$ ，若 $S\leq 0$ ，唤醒等待队列中的一个进程。

信号量、P 操作、V 操作的结合常见以下 4 种情况。

① 完成互斥控制。

也就是保护共享资源，不让多个进程同时访问这个共享资源，换句话说，就是阻止多个进程同时进入访问这些资源的代码段，这个代码段称为临界区（也称为管程），而这种一次仅允许一个进程访问的资源称为临界资源。对于临界区的代码就是：

```
P(信号量)
临界区
V(信号量)
```

由于只允许一个进程进入，因此信号量中整型值的初始值应该为 1。该值表示可以允许多少个进程进入。当该值小于 0 时，其绝对值就是等待使用的进程数，也就是等待队列中的进程数。而当一个进程从临界区出来时，就会将整型值加 1，如果等待队列中还有进程，则调入一个新的进程进入（唤醒）。

② 完成同步控制。

最简单的同步形式是：进程 A 在另一个进程 B 到达 L2 以前，不应前进到超过点 L1，这样就可以使用程序。

进程 A	进程 B
...	...
L1:P(信号量)	L2:V(信号量)
...	...

因此要确保进程 B 执行 V 操作之前，不让进程 A 的运行超过 L1，信号量的初始值就应该为 0。这样，如果进程 A 先执行到 L1，那么执行 P 操作后，信号量的整型值就会小于 1，也就停止执行。直到进程 B 执行到 L2 时，将信号量的整型值减 1，并唤醒它以继续执行。

③ 生产者-消费者问题。

生产者-消费者是一个经典的问题，它不仅要解决生产者进程与消费者进程的同步关系，还要处理缓冲区的互斥关系，因此通常需要三个信号量来实现。其中，两个用来管理同步：empty 信号量（说明空闲的缓冲区数量，最早没有产生东西，因此其初始值应为缓冲区的最大数）和 full 信号量（说明已填充的缓冲区数量，其初始值应为 0）。另一个 mutex 信号量用来管理互斥，以保证同时只有一个进程在写缓冲区（因此其初始值应为 1，参见“互斥控制的实现”）。

生产者	消费者
loop	loop
...	...
生产一个产品；	P(full)；
P(empty)；	P(mutex)；
P(mutex)；	从缓冲区中取一个产品；
将新产品放入缓冲区；	V(mutex)；
V(mutex)；	V(empty)；

```
V(full);          使用产品;
...              ...
endloop          endloop
```

注：如果对缓冲区的读/写无须进行互斥控制，那么就可以省去 **mutex** 信号量。

④ 阅读者和写入者问题。

假设有一个数据集被多个并行进程共享，其中有些进程只是读这个数据集，而有些进程则需要修改这个数据集的内容。这里存在着一个什么样的并发关系呢？阅读者相互不影响，但写入者则是互斥访问的。因此，解决这个问题最简单的方法是：当没有写入者在访问共享数据集时，阅读者可以进入访问，否则必须等待。下面则是一个读者优先的解法，其中信号量 **access** 用来控制写入互斥；而信号量 **rc** 则用来控制 **rc**（读者统计值）的互斥访问。

阅读者	写入者
loop	loop
P(rc)	...
ReaderCount=ReaderCount+1;	P(access);
If(ReaderCount==1)	修改数据;
P(access);	V(access);
V(rc);	...
访问数据;	endloop
P(rc);	
ReaderCount=ReaderCount-1;	
If(ReaderCount ==0)	
V(access);	
V(rc);	
...	
Endloop	

⑤ 理解 P、V 操作。

信号量与 P、V 操作的概念比较抽象，在历年的考试中总是难倒许多考生，其实主要还是没有能够正确地理解信号量的含义。

信号量与 P、V 操作是用来解决并发问题的，而在并发问题中最重要的是互斥与同步两个关系，也就是说，只要有这两个关系存在，信号量就有用武之地。因此，在解题时，应该先从寻找互斥与同步关系开始。这个过程可以套用简单互斥、简单同步、生产者-消费者、阅读者-写入者问题。

一般来说，一个互斥或一个同步关系可以使用一个信号量来解决，但要注意经常会忽略一些隐藏的同步关系。例如，在生产者-消费者问题中，就有两个同步关系，一是判断是否有足够的空间给生产者存放产物，另一个是判断是否有足够的内容让消费者使用。

信号量的初始值通常表示资源的可用数。而且对于初始值为 0 的信号量，通常会先做 V 操作。

在资源使用之前，将会使用 P 操作。在资源用完之后，将会使用 V 操作。在互斥关系中，P、V 操作是在一个进程中成对出现的。而在同步关系中，P、V 操作则一定是在两个进程甚至多个进程中成对出现的。

另外，值得一提的是，操作系统还提供了一些高级通信原语，如 Write/Read, Send/Receive 可以实现相同的功能，它们能够更好地补充 P、V 操作的不足，完成更多的功能。

(3) 进程死锁与银行家算法

进程管理是操作系统的核心，但如果设计不当，就会出现死锁的问题。如果一个进程在等待一个不可能发生的事，则进程就死锁了。而如果一个或多个进程产生死锁，就会造成系

系统死锁。

下面是造成系统死锁的 4 个必要条件。

① 互斥条件：即一个资源每次只能被一个进程使用，在操作系统中这是真实存在的情况。

② 保持和等待条件：有一个进程已获得了一些资源，但因请求其他资源被阻塞时，对已获得的资源保持不放。

③ 不可剥夺条件：有些系统资源是不可剥夺的，当某个进程已获得这种资源后，系统不能强行收回，只能由进程使用完时自己释放。

④ 环路等待条件：若干个进程形成环形链，每个都占用对方要申请的下一个资源。

对于这些内容，关键在于融会贯通地理解与应用，通常都会涉及银行家算法。所谓银行家算法，是指在分配资源之前，先看清楚，如果资源分配下去后，是否会导致系统死锁。如果会死锁，则不分配，否则就分配。为了帮助考生更好地理解，下面我们通过一个例子来说明银行家算法的应用。

假设系统中有三类互斥资源 R1、R2 和 R3，可用资源数分别是 9、8 和 5。在 T0 时刻系统中有 P1、P2、P3、P4 和 P5 共 5 个进程，这些进程对资源的最大需求量和已分配资源数如表 2-2 所示。

表 2-2 进程对资源的最大需求量和分配资源数

进程	资源	最大需求量			已分配资源数		
		R1	R2	R3	R1	R2	R3
P1		6	5	2	1	2	1
P2		2	2	1	2	1	1
P3		8	0	1	2	1	0
P4		1	2	1	1	2	0
P5		3	4	4	1	1	3

进程按照 P1→P2→P4→P5→P3 序列执行，系统状态安全吗？如果按 P2→P4→P5→P1→P3 的序列呢？

在这个例子中，我们先看一下未分配的资源还有哪些？很明显，还有 2 个 R1 未分配，1 个 R2 未分配，而 R3 全部分配完毕。

按照 P1→P2→P4→P5→P3 的顺序执行：

首先执行 P1，这时由于其 R1、R2 和 R3 的资源数都未分配够，因而开始申请资源，得到还未分配的 2 个 R1、1 个 R2。但其资源仍不足（没有 R3 资源），从而进入阻塞状态，并且这时所有资源都已经分配完毕。因此，后续的进程都无法得到能够完成任务的资源，全部进入阻塞状态，形成死循环，死锁发生了。

如果按照 P2→P4→P5→P1→P3 的序列执行：

首先执行 P2，它还差 1 个 R2 资源，系统中还有 1 个未分配的 R2，因此满足其要求，能够顺利结束进程，释放出 2 个 R1、2 个 R2、1 个 R3。这时，未分配的资源就是 4 个 R1、2 个 R2、1 个 R3。然后执行 P4，它还差一个 R3，而系统中刚好有一个未分配的 R3，因此满足其要求，也能够顺利结束，并释放出其资源。因此，这时系统就有 5 个 R1、4 个 R2、1 个 R3。

根据这样的方式推下去，会发现按这种序列可以顺利地完成任务，而不会出现死锁现象。从这个例子中，我们也可以体会到，死锁的 4 个条件是如何起作用的。只要打破任

何一个条件，就不会产生死锁。

在了解了进程死锁和银行家算法之后，接下来我们了解一下解决死锁的策略。

① 死锁预防：“解铃还需系铃人”，随便破坏导致死锁的任意一个必要条件就可以预防死锁。例如，要求用户申请资源时一次性申请所需要的全部资源，这样就破坏了保持和等待条件。将资源分层，得到上一层资源后，才能够申请下一层资源，它破坏了环路等待条件。预防通常会降低系统的效率。

② 死锁避免：避免是指进程在每次申请资源时判断这些操作是否安全，典型算法是银行家算法。但这种算法会增加系统的开销。

③ 死锁检测：前两者是事前措施，而死锁的检测则是判断系统是否处于死锁状态，如果是，则执行死锁解除策略。

④ 死锁解除：这是与死锁检测结合使用的，它使用的方式就是剥夺。即将某进程所拥有的资源强行收回，分配给其他进程。

2.2.2 一点一练

试题 1

在计算机系统中，构成虚拟存储器（1）。

- (1) A. 只需要一定的硬件资源即可实现 B. 只需要一定的软件即可实现
C. 既需要硬件也需要软件方可实现 D. 既不需要软件也不需要硬件

试题 2

进程是操作系统中一个重要的概念，它是一个具有一定独立功能的程序在某个数据（2）。

- (2) A. 单独操作 B. 关联操作 C. 运行活动 D. 并发活动

试题 3

若在系统中有若干个互斥资源 R，6 个并发进程中的每一个都需要两个资源 R，那么使系统不发生死锁 R 的最少数目为（3）。

- (3) A. 6 B. 7 C. 9 D. 12

试题 4

进程是一个（4）的概念。

- (4) A. 静态 B. 动态 C. 逻辑 D. 物理

试题 5

某系统的进程状态转换如图 2-4 所示，图中 1、2、3、4 分别表示引起状态转换的不同原因，原因 4 表示（5）。

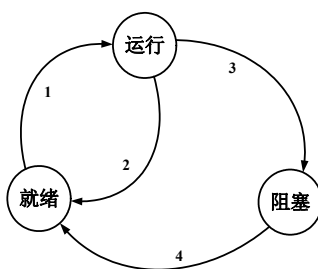


图 2-4 进程状态转换图

- (5) A. 就绪进程被调度
C. 发生了阻塞进程等待的事件

- B. 运行进程执行了 P 操作
D. 运行进程时间片到了

2.2.3 解析与答案

试题 1 分析

本题考查虚拟存储的构成。

虚拟存储器是操作系统自动实现存储信息调度和管理，但需要有硬件资源的配合实现。

主存的特点是速度快但容量小，CPU 可直访问。外存的特点是容量大和速度慢，CPU 不能直接访问。用户的程序和数据通常放在外存中。因此需要经常在主存与外存间取来送去。由用户来干预调度很不方便。虚拟存储器用来解决这个矛盾，使用户感到它可以直接访问整个内外存空间，而不需要用户干预。因此容量很大的速度较快的外存储器（硬磁盘）成为虚拟存储器主要组成部分。

虚拟存储器中硬盘中的数据 and 主存中的数据的调度方法与高速缓存 Cache 的调度方法类似。即把经常访问的数据调入高速主存中保存。不需要的数据用一定的替代算法再送回硬盘中。这些调入调出的操作都是由虚拟存储器自动完成的。

综上所述，构成虚拟存储器既需要硬件也需要软件。

试题 1 答案

(1) C

试题 2 分析

进程是操作系统中最基本的并行单位、资源分配单位和调度单位，通常可分为用户进程和系统进程。前者控制用户作业的运行，后者完成系统内部分工的管理工作。进程也是一个具有一定独立功能的程序在某个数据集合上的一次运行，其中可能要设计多个程序，而一个程序的运行过程总可能有若干进程依次或并行活动。

试题 2 答案

(2) C

试题 3 分析

本题要求限制进程申请的资源数来确保系统的安全。若要使系统不发生死锁，则应保证系统处于“安全状态”。也就是要保证所有的进程能在有限的时间中得到所需的资源。我们可以假设允许每个进程最多可以申请 x 个资源 ($1 \leq x \leq m$)，那么最坏的情况是每个进程都已得到 $x-1$ 个资源。现均要申请最后一个资源，因而只要系统至少还有一个资源又可供其他进程使用，就不可能发生死锁。也就是说，只要不等式 $n(x-1)+1 \leq m$ 成立，则系统一定不会发生死锁 (n 表示进程数， m 表示需要的资源数)。

结合题干的描述，现有 6 个并发进程，假设每个进程最多可以申请两个资源，为保证系统不发生死锁，应该使不等式 $6 \times (2-1) + 1 \leq m$ 。

解上述不等式即可知道 $m \geq 7$ 时，系统才不会出现死锁的现象。

试题 3 答案

(3) B

试题 4 分析

进程是一个动态的概念，程序是一个静态的概念。程序是指令的有序集合，没有任何执行的含义。进程则强调过程，它被动态创建，并在调度执行后消亡。程序好比是曲谱，而进

程就想是按照曲谱演奏的音乐。

试题 4 答案

(4) B

试题 5 分析

本题考查的是计算机操作系统进程管理方面的基础知识。图 2-4 中原因 1 是由于调度程序的调度引起；原因 2 是由于时间片用完引起；原因 3 是由于 I/O 请求引起，例如进程执行了 P 操作，由于申请的资源得不到满足进入阻塞队列；原因 4 是由于 I/O 完成引起的，例如某进程执行了 V 操作将信号量值加 1，若信号量的值小于等于 0，意味着有等待该资源的进程，将该进程从阻塞队列中唤醒使其进入就绪队列。正确答案是 C。

试题 5 答案

(5) C

2.3 文件管理

文件管理是对外部存储设备上、以文件方式存放的信息的管理。从历年试题来看，主要集中在文件的组织和结构试题上。

2.3.1 考点精讲

文件的结构是指文件的组织形式，又称为“文件的逻辑结构”。文件控制块的集合称为文件目录，当前流行的 UNIX、Windows 系统都采用多级树型目录结构。

1. 文件组织结构

本节简单介绍文件的结构、访问方式和控制块等基本概念。

(1) 文件的结构

文件的结构是指文件的组织形式，从用户观点所看到的文件组织形式，称为文件的逻辑结构。一般文件的逻辑结构可以分为两种，分别是无结构的字符流文件和有结构的记录文件。记录文件由记录组成，即文件内的信息划分成多个记录，以记录为单位组织和使用信息。记录文件有顺序文件、索引顺序文件、索引文件和直接文件。

文件的物理结构是指文件在存储设备上的存放方法。文件的物理结构侧重于提高存储器的利用效率和降低存取时间。文件的存储设备通常划分为大小相同的物理块，物理块是分配和传输信息的基本单位。文件的物理结构涉及文件存储设备的组织策略和文件分配策略，决定文件信息在存储设备上的存储位置。常用的文件分配策略有顺序分配（连续分配）、链接分配（串联分配）、索引分配。

(2) 文件的访问方式

用户通过对文件的访问（读/写）来完成对文件的查找、修改、删除和添加等操作。常用的访问方法有两种，即顺序访问和随机访问。

(3) 文件控制块

文件控制块是系统在管理文件时所必需的信息的数据结构，是文件存在的唯一标志，简称 FCB。文件目录就是文件控制块的有序集合。FCB 的内容包括相应文件的基本属性，大致可以分成 4 个部分。

- ① 基本信息：如文件名、文件类型和文件组织等。
- ② 保护信息：如口令、所有者名、保存期限和访问权限等。
- ③ 位置信息：如存储位置、文件长度等。

④ 使用信息：如时间信息、最迟使用者等。

(4) 树型目录结构

文件控制块的集合称为文件目录，文件目录也被组织成文件，常称为目录文件。文件管理的一个重要方面是对文件目录进行组织和管理。文件系统一般采用一级目录结构、二级目录结构和多级目录结构。DOS、UNIX、Windows 系统都采用多级树型目录结构。

在多级树型目录结构中，整个文件系统有一个根，然后在根上分枝，任何一个分枝上都可以再分枝，枝上也可以长出树叶。根和枝称为目录或文件夹。而树叶则是一个个的文件。实践证明，这种结构的文件系统效率比较高。例如，如图 2-5 所示的就是一个树型目录结构，其中方框代表目录，圆形代表文件。

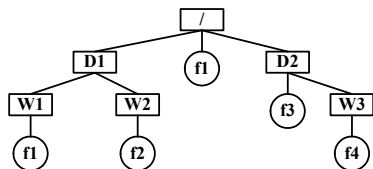


图 2-5 树型文件结构

在树型目录结构中，树的根节点为根目录，数据文件作为树叶，其他所有目录均作为树的节点。系统在建立每一个目录时，都会自动为它设定两个目录文件，一个是“.”，代表该目录自己；另一个是“..”，代表该目录的父目录。对于根目录，“.”和“..”都代表其自己。

从逻辑上讲，用户在登录到系统之后，每时每刻都处在某个目录之中，此目录被称作工作目录或当前目录。工作目录是可以随时改变的。

对文件进行访问时，需要用到路径的概念。路径是指从树型目录中的某个目录层次到某个文件的一条道路。在树型目录结构中，从根目录到任何数据文件之间，只有一条唯一的通路，从树根开始，把全部目录文件名与数据文件名依次用“/”连接起来，构成该数据文件的路径名，且每个数据文件的路径名是唯一的。这样，可以解决文件重名问题，不同路径下的同名文件不一定是相同的文件。例如，在图 2-5 中，根目录下的文件 f1 和/D1/W1 目录下的文件 f1 可能是相同的文件，也可能是不相同的文件。

用户在对文件进行访问时，要给出文件所在的路径。路径又分相对路径和绝对路径。绝对路径是指从根目录开始的路径，也称为完全路径；相对路径是指从用户工作目录开始的路径。应该注意到，在树型目录结构中到某一确定文件的绝对路径和相对路径均只有一条。绝对路径是确定不变的，而相对路径则随着用户工作目录的变化而不断变化。

用户要访问一个文件时，可以通过路径名来引用。例如，在图 2-5 中，如果当前路径是 D1，则访问文件 f2 的绝对路径是/D1/W2/f2，相对路径是 W2/f2。如果当前路径是 W1，则访问文件 f2 的绝对路径仍然是/D1/W2/f2，但相对路径变为../W2/f2。

在 Windows 系统中，有两种格式的文件，分别是 FAT32（FAT16）文件和 NTFS 文件。NTFS 在使用中产生的磁盘碎片要比 FAT32 少，安全性也更高，而且支持单个文件的容量更大，超过了 4GB，特别适合现在的大容量存储。NTFS 可以支持的分区（如果采用动态磁盘则称为卷）大小可以达到 2TB。

2.3.2 一点一练

试题 1

若文件系统允许不同用户的文件可以具有相同的文件名，则操作系统应采用（1）来

实现。

- (1) A. 索引表 B. 索引文件 C. 指针 D. 多级目录

试题 2

操作系统是裸机上的第一层软件，其他系统软件（如____(2)____等）和应用软件都是建立在操作系统基础上的。图 2-6，①②③分别表示____(3)____。

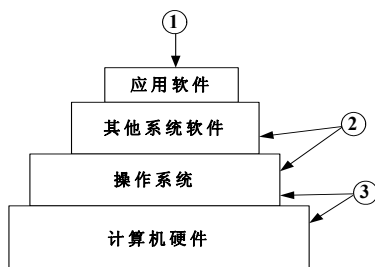


图 2-6 软件层次图

- (2) A. 编译程序、财务软件和数据库管理系统软件
B. 汇编程序、编译程序和 Java 解释器
C. 编译程序、数据库管理系统软件和汽车防盗程序
D. 语言处理程序、办公管理软件和气象预报软件
- (3) A. 应用软件开发者、最终用户和系统软件开发者
B. 应用软件开发者、系统软件开发者和最终用户
C. 最终用户、系统软件开发者和应用软件开发者
D. 最终用户、应用软件开发者和系统软件开发者

试题 3

在操作系统文件管理中，通常采用____(4)____来组织和管理外存中的信息。

- (4) A. 字处理程序 B. 设备驱动程序 C. 文件目录 D. 语言翻译程序

试题 4

若某文件系统的目录结构如图 2-7 示，假设用户要访问文件 f1.java，且当前工作目录为 Program，则该文件的全文件名为____(5)____。

- (5) A. f1.java B. \Document\java-prog\f1.java
C. D:\Program\java-prog\f1.java D. \Program\Java-prog\f1.java

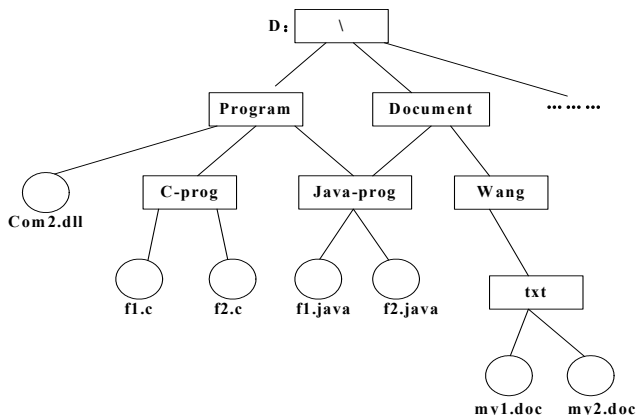


图 2-7 目录树结构

试题 5

NTFS 文件系统中要求用户可以创建新文件、修改文件内容，但不可以删除文件，则应采用的 NTFS 权限是 (6)。

(6) A. 完全控制 B. 修改 C. 改变 D. 写

2.3.3 解析与答案

试题 1 分析

文件系统把所有文件的文件目录放在一个特殊的文件中，这个全部由文件目录项组成的文件称为“目录文件”，它为文件管理提供了重要的依据。目前常用的目录机构形式有单级和多级目录。由于所有文件都在一个目录文件中，则对所有系统中文件数增多时查找时间也相应增大，使搜索速度减慢。如果文件重名，对使用文件会造成影响。因此单级目录结构只适合于较小的文件系统。多级目录也称为“树型目录结构”，其中将第一级作为系统根目录，称为“目录树的根节点”。其他各级中的目录都是这个目录树的分支节点，统称“子目录”。多级目录很好地解决了文件重名的问题。

试题 1 答案

(1) D

试题 2 分析

本题考查操作系统基本概念。

财务软件、汽车防盗程序、办公管理软件和气象预报软件都属于应用软件，而选项 A、C 和 D 中含有这些软件。选项 B 中汇编程序、编译程序和数据库管理系统软件都属于系统软件。

计算机系统由硬件和软件两部分组成。通常把未配置软件的计算机称为裸机，直接使用裸机不仅不方便，而且将严重降低工作效率和机器的利用率。操作系统 (Operating System) 的目的是为了填补人与机器之间的鸿沟，即建立用户与计算机之间的接口而为裸机配置的一种系统软件。由图 2-6 可以看出，操作系统是裸机上的第一层软件，是对硬件系统功能的首次扩充。它在计算机系统中占据重要而特殊的地位，所有其他软件，如编辑程序、汇编程序、编译程序和数据库管理系统等系统软件，以及大量的应用软件都在操作系统基础上的，并得到它的支持和取得它的服务。从用户角度看，当计算机配置了操作系统后，用户不再直接使用计算机系统硬件，而是利用操作系统所提供的命令和服务去操纵计算机，操作系统已成为现代计算机系统中必不可少的最重要的系统软件，因此把操作系统看作用户与计算机之间的接口。因此，操作系统紧贴系统硬件之上，所有其他软件之下（是其他软件的共同环境）。

试题 2 答案

(2) B (3) D

试题 3 分析

本题考查的是操作系统文件管理方面的基础知识。

存放在磁盘空间上的各类文件必须进行编目，操作系统才能实现文件的管理，这与图书馆中的藏书需要编目录、一本书需要分章节是类似的。用户总是希望能“按名存取”文件中的信息。为此，文件系统必须为每一个文件建立目录项，即为每个文件设置用于描述和控制文件的数据结构，记载该文件的基本信息，如文件名、文件存放的位置、文件的物理结构等。这个数据结构称为文件控制块 FCB，文件控制块的有序集合称为文件目录。

试题 3 答案

(4) C

试题 4 分析

本题考查 Windows 操作系统中的文件目录结构。

在对数据文件进行操作时，一般要用盘符指出被操作的文件或目录在哪一磁盘。盘符也称驱动器名。

文件是按一定格式建立在外存储介质上的一组相关信息的集合。计算机中的文件一般存储在磁盘、光盘或磁带中，如果没有特殊说明，我们认为文件是存储在磁盘上的，称为磁盘文件。每一个文件必须有一个名字，称为文件名。

文件目录，即 Windows 操作系统中的文件夹。为了实现对文件的统一管理，同时又方便用户，操作系统采用树状结构的目录来实现对磁盘上所有文件的组织和管理。根目录用“\”表示，从根目录或当前目录至所要找的文件或目录所需要经过的全部子目录的顺序组合。

绝对路径指的是从根目录开始到目标文件或目录的一条路径。所以 fl.java 文件的绝对路径是“D:\Program\java-prog\fl.java”。

试题 4 答案

(5) C

试题 5 分析

此题考查的是 NTFS 权限。根据题干需求，赋予相应用户对该文件夹具有写权限即可。写就相当于可以实现创建新文件，修改文件内容，但是不能删除文件的权限组合。

试题 5 答案

(6) D

2.4 考前冲刺

试题 1

不属于进程三种基本状态的是____(1)____。

(1) A. 运行态 B. 就绪态 C. 后备态 D. 阻塞态

试题 2

在一个单处理机中若有 6 个用户进程，在非管态的某一个时刻处于就绪状态的用户进程最多有____(2)____个。

(2) A. 5 B. 0 C. 1 D. 4

试题 3

以下不属于操作系统基本功能的是____(3)____。

(3) A. 进程管理 B. 作业管理 C. 内部管理 D. 存储管理

试题 4

系统中有 R 类资源 m 个，现有 n 个进程互斥使用。若每个进程对 R 资源的最大需求为 w ，那么当 m 、 n 、 w 取下表的值时，对于表 2-3 中的 a~e 5 种情况，____(4)____两种情况可能会发生死锁。

表 2-3 系统资源分配表

	a	b	c	d	e
m	2	2	2	4	4
n	1	2	2	3	3
w	2	1	2	2	3

- (4) A. a 和 b B. b 和 c C. c 和 d D. c 和 e

试题 5

进程 Pa 不断向管道写数据，进程 Pb 从管道中读取数据并加工处理，如图 2-8 所示。如果采用 PV 操作来实现进程 Pa 和 Pb 的管道通信，并且保证这两个进程并发执行的正确性，则至少需要____(5)_____。

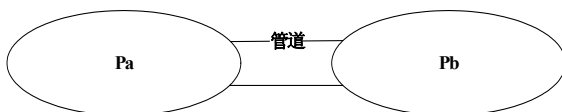


图 2-8 进程 Pa 和 Pb

- (5) A. 1 个信号量，信号量的初始值为 0
 B. 2 个信号量，信号量的初始值为 0、1
 C. 3 个信号量，信号量的初始值为 0、0、1
 D. 4 个信号量，信号量的初始值为 0、0、1、1

试题 6

因争用资源产生死锁的必要条件是互斥、循环等待、不可抢占和____(6)_____。

- (6) A. 请求与释放 B. 释放与等待
 C. 释放与阻塞 D. 保持与等待

试题 7

页式虚拟存储系统的逻辑地址是由页号和页内地址两部分组成，地址变换过程如图 2-9 所示。假定页面的大小为 8K，图中所示的十进制逻辑地址 9612 经过地址变换后，形成的物理地址 a 应为十进制____(7)_____。

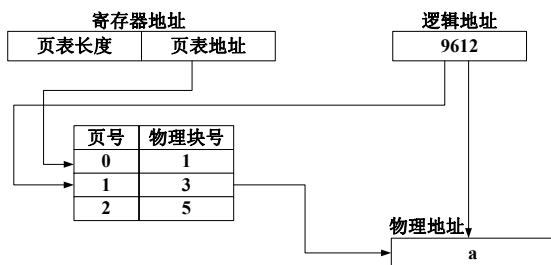


图 2-9 虚存地址变换图

- (7) A. 42380 B. 25996 C. 9612 D. 8192

试题 8

内存采用段式存储管理有许多优点，但____(8)_____不是其优点。

- (8) A. 分段是信息逻辑单位，用户不可见 B. 各段程序的修改互不影响
 C. 地址变换速度快、内存碎片少 D. 便于多道程序共享主存的某些段

试题 9

采用生产者和消费者方式解决同步和互斥时通常需要用____(9)_____个信号量。

- (9) A. 1 B. 2 C. 3 D. 4

试题 10

以下不属于常见的虚存组织技术的是____(10)_____。

(10) A. 段式虚存管理 B. 页式虚存管理 C. 段页式虚存管理 D. 块式虚存管理

2.5 习题解析

试题 1 分析

进程在运行中不断地改变其运行状态。通常,一个运行进程必须具有以下三种基本状态。

就绪(Ready)状态:当进程已分配到除 CPU 以外的所有必要的资源,只要获得处理机便可立即执行,这时的进程状态称为就绪状态。

执行(Running)状态:当进程已获得处理机,其程序正在处理机上执行,此时的进程状态称为执行状态。

阻塞(Blocked)状态:正在执行的进程,由于等待某个事件发生而无法执行时,便放弃处理机而处于阻塞状态。引起进程阻塞的事件可有多种,例如,等待 I/O 完成、申请缓冲区不能满足、等待信件(信号)等。

试题 1 答案

(1) C

试题 2 分析

在一个单处理机中只有一个处理器,非管态(即用户进程执行状态)的某一时刻处于运行状态的进程至少且最多只有一个;处于就绪或阻塞状态的进程可能有多个,这样处于就绪态的进程数最多只能是进程总数减 1。如果除了运行态的一个进程外,其余进程均处于阻塞态,则就绪态的进程个数为 0。

试题 2 答案

(2) A

试题 3 分析

操作系统提供了 5 个方面的功能:进程管理、文件管理、存储管理、设备管理和作业管理。处理机管理是对处理机的执行“时间”进行管理。通过进程管理协调多道程序之间的关系,解决对处理器实施分配调度策略、进行分配和进行回收等问题,以使 CPU 资源得到最充分的利用。文件管理主要包括存储分配与回收、存储保护、地址映射和主存扩充。存储管理是对主存储器“空间”进行管理。设备管理是对硬件设备的管理,设备管理不仅涵盖了进行实际 I/O 操作的设备,还涵盖了例如设备控制器、通道等输入/输出支持设备。作业管理包括任务、界面管理、人机交互、语音控制等。

试题 3 答案

(3) C

试题 4 分析

本题考查对操作系统死锁方面基本知识掌握的程度。系统中同类资源分配不当会引起死锁。一般情况下,若系统中有 m 个单位的存储器资源,它被 n 个进程使用,当每个进程都要求 w 个单位的存储器资源,当 $m > nw$ 时,可能会引起死锁。

情况 a: $m=2, n=1, w=2$, 系统中有 2 个资源,1 个进程使用,该进程最多要求 2 个资源,所以不会发生死锁。

情况 b: $m=2, n=2, w=1$, 系统中有 2 个资源,2 个进程使用,每个进程最多要求 1 个资源,所以不会发生死锁。

情况 c: $m=2, n=2, w=2$, 系统中有 2 个资源,2 个进程使用,每个进程最多要求 2 个资源,此时,采用的分配策略是轮流地为每个进程分配,则第一轮系统先为每个进程分配 1

个，此时，系统中已无可供分配的资源，使得各个进程都处于等待状态导致系统发生死锁。

情况 d: $m=4$, $n=3$, $w=2$ ，系统中有 4 个资源，3 个进程使用，每个进程最多要求 2 个资源，此时，采用的分配策略是轮流地为每个进程分配，则第一轮系统先为每个进程分配 1 个资源，此时，系统中还剩 1 个资源，可以使其中的一个进程得到所需资源并运行完毕，所以不会发生死锁。

情况 e: $m=4$, $n=3$, $w=3$ ，系统中有 4 个资源，3 个进程使用，每个进程最多要求 3 个资源，此时，采用的分配策略是轮流地为每个进程分配，则第一轮系统先为每个进程分配 1 个，第二轮系统先为一个进程分配 1 个，此时，系统中已无可供分配的资源，使得各个进程都处于等待状态导致系统发生死锁。

试题 4 答案

(4) D

试题 5 分析

这是一个典型的生产者和消费者问题。其中进程 Pa 和 Pb 分别为生产者和消费者，管道为临界区。我们的程序应该设置一个同步信号量，为 1 时说明管道已满拒绝 Pa 再写入数据；为 0 时说明管道为空拒绝 Pb 再读出数据。管道初始是没有数据的，所以初始值为 0（特殊情况即管道的大小为 1 个单位）。程序还需要 1 个互斥信号量来保证程序只有一个进程访问管道，其初始值为 1。

试题 5 答案

(5) B

试题 6 分析

本题主要考查进程管理中有关死锁的知识点。当有多个任务竞争同样的两个或多个临界资源时会出现死锁，产生死锁的必要条件是互斥、不可抢占、保持与等待、循环等待。

试题 6 答案

(6) D

试题 7 分析

本题考查页式存储管理中的地址变换知识。在页式存储管理中，有效地址除以页的大小，取整为页号，取余为页内地址。本题页面的大小为 8KB，有效地址 9612 除以 8192，取整为 1，取余为 1420。我们先查页表得物理块号 3，因此有效地址 a 为 $8192 \times 3 + 1420 = 25996$ 。

试题 7 答案

(7) B

试题 8 分析

本题考查操作系统内存管理方面的基本概念。操作系统内存管理方案有许多种，其中，分页存储管理系统中的每一页只是存放信息的物理单位，其本身没有完整的意义，因而不便于实现信息的共享，而段却是信息的逻辑单位，各段程序的修改互不影响，无内碎片，有利于信息的共享。

试题 8 答案

(8) C

试题 9 分析

当采用生产者与消费者方式解决同步和互斥时通常需要两个私用信号量，即 empty 和 full，以及一个公用信号量 mutex。其中 empty 表示空缓冲区数目的信号量。full 是表示满缓

缓冲区数目的信号量。**mutex** 是对临界缓冲区进行操作的互斥信号量。

试题 9 答案

(9) C

试题 10 分析

本题考查虚存管理方面的基础知识。

虚存管理中最常见的虚存组织有分段技术、分页技术、段页式技术 3 种，但没有块式虚存管理。

试题 10 答案

(10) D

计算机系统开发基础

计算机系统开发基础对于了解系统软件开发的流程、周期、所用技术、开发模型等知识点具有非常重要的作用。

3.1 考点脉络

系统开发基础是网络工程师考试中一个必考的内容。根据考试大纲,要求考生掌握以下几个方面的内容。

- (1) 系统开发模型: 包括瀑布模型、增量模型、原型模型等。
- (2) 需求分析: 包括需求分析任务、过程。
- (3) 软件设计: 包括耦合和内聚的概念、软件设计的过程、结构化设计思想等。
- (4) 软件测试: 包括测试阶段、测试类型、测试方法。
- (5) 项目管理: 包括项目管理工具、质量管理、CMM、关键路径等。

从历年的考试试题来看,本章的考点在综合知识考试中的平均分数为 3.5 分,约为总分的 5%。考试试题分数主要集中在系统开发模型、软件测试、项目管理基础知识这 3 个知识点上。

3.2 系统开发基础

在系统开发基础这个考点中,主要涉及系统开发模型、需求分析、软件设计、软件测试 4 个方面的内容。

3.2.1 考点精讲

软件开发模型(Software Development Model)是指软件开发全部过程、活动和任务的结构框架。软件开发模型的选取,对于大型信息管理系统开发成败起到至关重要的作用。软件需求分析就是把软件计划期间建立的软件可行性分析求精和细化,分析各种可能的解法,并且分配给各个软件元素。需求分析是软件定义阶段中的最后一步,是确定系统必须完成哪些工作,也就是对目标系统提出完整、准确、清晰、具体的要求。软件设计是把软件需求变换为软件表示的过程,可将软件设计分为概要设计和详细设计。软件测试是为了发现错误和执行程序的过程,也是为了保证系统的质量和可靠性。

1. 系统开发生命周期模型

在开发模型知识点中,我们要掌握软件生命周期的概念、各种开发模型的特点和应用场合。主要的开发模型及方法有瀑布模型、演化模型、螺旋模型、喷泉模型、智能模型、V 模型、增量模型、RAD 模型、原型方法等。

(1) 生命周期概述

系统开发生命周期是指一个系统历经计划、分析、设计、编程、测试、维护直至淘汰的整个过程。

生命周期阶段划分有如下 3 种方法。

① **Boehm 划分法**：计划（问题定义、可行性研究）、开发（需求分析、总体设计、详细设计、编码、测试）、运行（维护）三大阶段。

② **国标（GB 8566-1988）划分法**：可行性研究与计划、需求分析、概念设计、详细设计、实现、组装测试、确认测试、使用和维护，并在《GB/T 8566-1995 信息技术——软件生存期过程》中定义了获取过程、供应过程、开发过程、运行过程、维护过程、管理过程、支持过程 7 个部分。

③ **RUP 划分法**：分为初始、细化、构造、移交 4 个主要阶段。

(2) 生命周期模型

本节对一些主要的开发模型和方法进行简单的介绍。

① 瀑布模型

瀑布模型也称为生命周期法，是生命周期法中最常用的开发模型，它把软件开发的过程分为软件计划、需求分析、软件设计、程序编码、软件测试和运行维护 6 个阶段，规定了它们自上而下、相互衔接的固定次序，如同瀑布流水，逐级下落。采用瀑布模型的软件过程如图 3-1 所示。

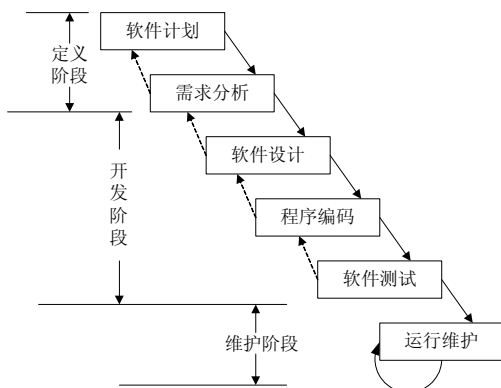


图 3-1 瀑布模型图

a. 软件计划（问题的定义及规划）：主要确定软件的开发目标及其可行性。

b. 需求分析：在确定软件开发可行的情况下，对软件需要实现的各个功能进行详细分析。需求分析阶段是一个很重要的阶段，这一阶段做得好，将为整个软件开发项目的成功打下良好的基础。

c. 软件设计：主要根据需求分析的结果，对整个软件系统进行设计，如系统框架设计、数据库设计等。软件设计一般分为总体设计（概要设计）和详细设计。

d. 程序编码：将软件设计的结果转换成计算机可运行的程序代码。在程序编写中必须要制定统一、符合标准的编写规范，以保证程序的可读性、易维护性，提高程序的运行效率。

e. 软件测试：在软件设计完成后要经过严密的测试，以发现软件在整个设计过程中存在的问题并加以纠正。在测试过程中需要建立详细的测试计划并严格按照测试计划进行测试，以减少测试的随意性。

f. 运行维护：运行维护是软件生命周期中持续时间最长的阶段。

瀑布模型是最早出现的软件开发模型，在软件工程中占有重要的地位，它提供了软件开发的基本框架。瀑布模型的本质是“一次通过”，即每个活动只做一次，最后得到软件产品，也称为“线性顺序模型”或者“传统生命周期”，其过程是从上一项活动接收该项活动的工作对象作为输入，利用这一输入实施该项活动应完成的内容，给出该项活动的工作成果，作为输出传给下一项活动；对该项活动实施的工作进行评审，若其工作得到确认，则继续下一项活动，否则返回前项，甚至更前项的活动进行返工。

瀑布模型有利于大型软件开发过程中人员的组织与管理,有利于软件开发方法和工具的研究与使用,从而提高了大型软件项目开发的质量和效率。然而软件开发的实践表明,上述各项活动之间并非完全是自上而下的,而是呈线性图式,因此,瀑布模型存在严重的缺陷。

a. 由于开发模型呈线性，所以当开发成果尚未经过测试时，用户无法看到软件的效果。这样，软件与用户见面的时间间隔较长，也增加了一定的风险。

b. 在软件开发前期未发现的错误传到后面的开发活动中时，可能会扩散，进而可能会导致整个软件项目开发失败。

c. 在软件需求分析阶段，完全确定用户的所有需求是比较困难的，甚至可以说是不太可能的。

② 演化模型

演化模型（变换模型）是在快速开发一个原型的基础上，根据用户在调用原型的过程中提出的反馈意见和建议，对原型进行改进，获得原型的新版本，重复这一过程，直到演化成为最终的软件产品。

③ 螺旋模型

螺旋模型将瀑布模型和变换模型相结合，它综合了两者的优点，并增加了风险分析。它以原型为基础，沿着螺线自内向外旋转，每旋转一圈都要经过制订计划、风险分析、实施工程、客户评价等活动，并开发原型的一个新版本。经过若干次螺旋上升的过程，得到最终的系统，如图 3-2 所示。

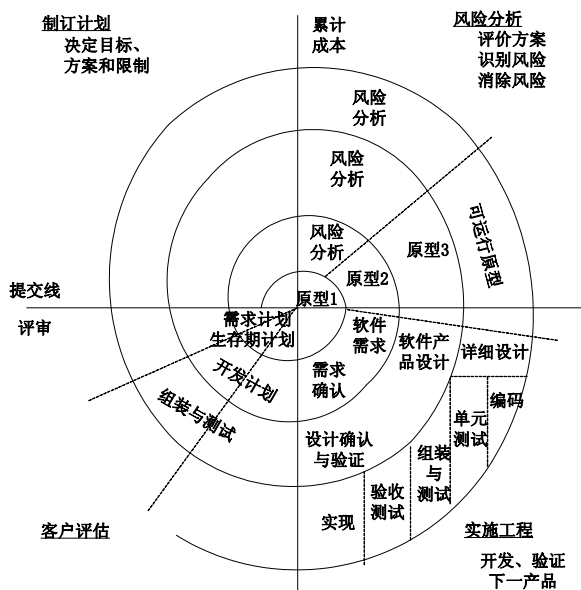


图 3-2 螺旋模型图

④ 喷泉模型

喷泉模型对软件复用和生命周期中多项开发活动的集成提供了支持，主要支持面向对象的开发方法。“喷泉”一词本身体现了迭代和无缝隙特性。系统某个部分常常重复工作多次，相关功能在每次迭代中随之加入演进的系统。所谓无缝隙是指在开发活动中，分析、设计和编码之间不存在明显的边界，如图 3-3 所示。

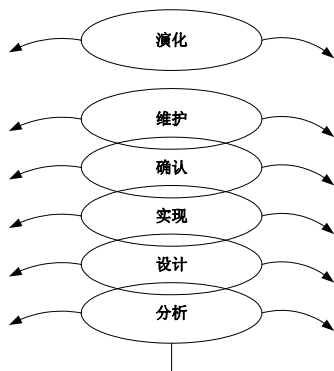


图 3-3 喷泉模型图

⑤ 智能模型

智能模型是基于知识的软件开发模型，它综合了上述若干模型，并把专家系统结合在一起。该模型应用基于规则的系统，采用归约和推理机制，帮助软件人员完成开发工作，并使维护在系统规格说明一级进行。

⑥ V 模型

在开发模型中，测试常常作为亡羊补牢的事后行为，但也有以测试为中心的开发模型，那就是 V 模型。V 模型只得到软件业内比较模糊的认可。V 模型宣称测试并不是一个事后弥补行为，而是一个与开发过程同样重要的过程，如图 3-4 所示。

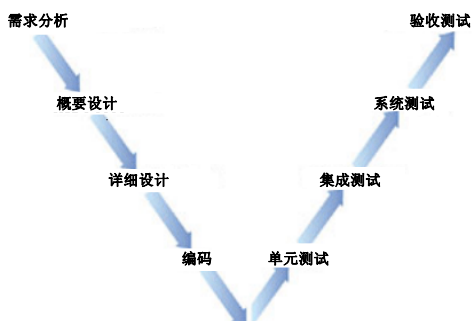


图 3-4 V 模型图

V 模型描述了一些不同的测试级别，并说明了这些级别所对应的生命周期中不同的阶段。在图 3-4 中，左边下降的是开发过程各阶段，与此相对应的是右边上升的部分，即测试过程的各个阶段。请注意在不同的组织中，对测试阶段的命名可能有所不同。

V 模型的价值在于它非常明确地标明了测试过程中存在的不同级别，并且清楚地描述了这些测试阶段和开发过程期间各阶段的对应关系。

a. 单元测试主要针对编码过程中可能存在的各种错误。例如，用户输入验证过程中边界值的错误。

b. 集成测试主要针对详细设计中可能存在的问题，尤其是检查各单元与其他程序部分之间的接口上可能存在的错误。

c. 系统测试主要针对概要设计，检查系统作为一个整体是否有效地得到运行。例如，在产品设置中是否达到了预期的高性能。

d. 验收测试通常由业务专家或用户进行，以确认产品能真正符合用户业务上的需要。

⑦ 增量模型

增量模型融合了瀑布模型的基本成分（重复的应用）和原型实现的迭代特征。增量模型采用随着时间的进展而交错的线性序列，每一个线性序列产生软件的一个可发布的“增量”。当使用增量模型时，第一个增量往往是核心的产品，也就是说，第一个增量实现了基本的需求，但很多补充的特征还没有发布。客户对每一个增量的使用和评估，都作为下一个增量发布的新特征和功能。这个过程在每一个增量发布后不断重复，直到产生最终的完善产品。增量模型强调每一个增量均发布一个可操作的产品。

增量模型像原型实现模型和其他演化方法一样，本质上是迭代的。但与原型实现不同的是，增量模型强调每一个增量均发布一个可操作产品。早期的增量是最终产品的“可拆卸”版本，但它们确实提供了为用户服务的功能，并且提供了给用户评估的平台。增量模型的特点是引进了增量包的概念，无须等到所有需求都出来，只要某个需求的增量包出来即可进行开发。虽然某个增量包可能还需要进一步适应客户的需求，还需要更改，但只要这个增量包足够小，其影响对整个项目来说是可以承受的。

采用增量模型的优点是人员分配灵活，刚开始不用投入大量人力资源，如果核心产品很受欢迎，则可以增加人力实现下一个增量；当配备的人员不能在设定的期限内完成产品时，它提供了一种先推出核心产品的途径，这样就可以先发布部分功能给客户，对客户起到镇静剂的作用。此外，增量能够有计划地管理技术风险。增量模型的缺点是如果增量包之间存在相交的情况且不能很好地处理，就必须做全盘的系统分析。增量模型将功能细化、分别开发的方法适用于需求经常改变的软件开发过程中。

⑧ RAD 模型

快速应用开发（Rapid Application Development, RAD）模型是一个增量型的软件开发过程模型，强调极短的开发周期。RAD 模型是瀑布模型的一个“高速”变种，通过大量使用可复用构件，采用基于构件的建造方法赢得快速开发。如果需求理解得好且约束了项目的范围，利用这种模型可以很快地创建出功能完善的“信息系统”。其流程从业务建模开始，随后是数据建模、过程建模、应用生成、测试及反复。

与瀑布模型相比，RAD 模型不采用传统的第三代程序设计语言来创建软件，而是采用基于构件的开发方法，复用已有的程序结构（如果可能的话）或使用可复用构件，或创建可复用的构件（如果需要的话）。在所有情况下，均使用自动化工具辅助软件创造。很显然，加在一个 RAD 模型项目上的时间约束需要“一个可伸缩的范围”。如果一个业务能够被模块化，使得其中每一个主要功能均可以在不到三个月的时间内完成，那么它就是 RAD 的一个候选者。每一个主要功能可由一个单独的 RAD 组来实现，最后再集成起来形成一个整体。

RAD 模型通过大量使用可复用构件加快了开发速度，对信息系统的开发特别有效。但是像所有其他软件过程模型一样，RAD 方法也有其缺陷。

a. 并非所有应用都适合 RAD。RAD 模型对模块化要求比较高，如果有哪一项功能不能被模块化，那么建造 RAD 所需要的构件就会有问题；如果高性能是一个指标，且该指标必须通过调整接口使其适应系统构件才能赢得，RAD 方法也有可能不能奏效。

b. 开发者和客户必须在很短的时间内完成一系列的需求分析，任何一方配合不当都会导致 RAD 项目失败。

c. RAD 只能用于信息系统开发，不适合技术风险很高的情况。当一个新应用要采用很多新技术或当新软件要求与已有的计算机程序有较高的互操作性时，这种情况就会发生。

⑨ 基于构件的模型

基于构件的软件开发（Component Based Software Development, CBSD）模型是利用模块化方法，将整个系统模块化，并在一定构件模型的支持下，复用构件库中的一个或多个软件构件，通过组合手段高效率、高质量地构造应用软件系统的过程。基于构件的开发模型融合了螺旋模型的许多特征，本质上是演化型的，开发过程是迭代的。基于构件的开发模型由软件的需求分析和定义、体系结构设计、构件库建立、应用软件构建、测试和发布 5 个阶段组成。采用基于构件的开发模型的软件过程如图 3-5 所示。

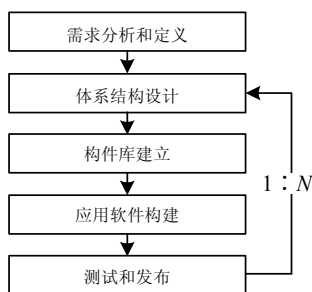


图 3-5 采用基于构件的开发模型的软件过程模型图

构件作为重要的软件技术和工具得到了极大的发展，这些新技术和工具有 Microsoft 的 DCOM、Sun 的 EJB、OMG 的 CORBA 等。基于构件的开发活动从标识候选构件开始，通过搜查已有构件库，确认所需要的构件是否已经存在，如果已经存在，就从构件库中提取出来复用；如果不存在，就采用面向对象方法开发它。在提取出来的构件通过语法和语义检查后，将这些构件通过胶合代码组装到一起实现系统，这个过程是迭代的。

基于构件的开发方法使得软件开发不再一切从头开发，开发的过程就是构件组装的过程，维护的过程就是构件升级、替换和扩充的过程，其优点是构件组装模型导致了软件的复用，提高了软件开发的效率；构件可由一方定义其规格说明，被另一方实现，然后供给第三方使用，构件组装模型允许多个项目同时开发，降低了费用，提高了可维护性，可实现分步提交软件产品。缺点是由于采用自定义的组装结构标准，缺乏通用的组装结构标准，引入具有较大的风险；可重用性和软件高效性不易协调，需要精干的、有经验的分析人员和开发人员，一般的开发人员插不上手，客户的满意度低；过分依赖于构件，构件库的质量影响着产品质量。

⑩ 原型方法

软件原型是所提出的新产品的部分实现，建立原型的主要目的是为了解决在产品开发的早期阶段需求不确定的问题，其作用是明确并完善需求，探索设计选择方案，发展为最终的产品。

原型有很多种分类方法。从原型是否实现功能来分，软件原型可分为水平原型和垂直原型两种。水平原型也称为行为原型，用来探索预期系统的一些特定行为，并达到细化需求的目的。水平原型通常只是功能的导航，但并未真实实现功能。水平原型主要用在界面上。垂直原型也称为结构化原型，实现了一部分功能。垂直原型主要用在复杂的算法实现上。

从原型的最终结果来分，软件原型可分为抛弃型原型和演化型原型。抛弃型原型也称为探索型原型，是指达到预期目的后，原型本身被抛弃。抛弃型原型主要用在解决需求不确定性、二义性、不完整性、含糊性等方面。演化型原型为开发增量式产品提供基础，是螺旋模型的一部分，也是面向对象软件开发过程的一部分。演化型原型主要用在必须易于升级和优化方面，适用于 Web 项目。

有些文献把原型分为探索型、实验型和演化型。探索型原型的目的是要弄清对目标系统

的要求,确定所希望的特性,并探讨多种方案的可行性。实验型原型用于大规模开发和实现之前,考核方案是否合适,规格说明是否可靠。演化型原型的目的在于改进规格说明,而是将系统建造得易于变化,在改进原型的过程中,逐步将原型进化成最终系统。

原型法适合于用户没有肯定其需求的明确内容的时候。它是先根据已给的和分析的需求,建立一个原始模型,这是一个可以修改的模型(在生命周期法中,需求分析成文档后一般不再做修改)。在软件开发的各个阶段都相互反馈有关信息,直至模型的修改使模型渐趋完善。在这个过程中,用户的参与和决策加强了,最终的结果是更适合用户的要求。这种原型技术又分为三类:抛弃式、演化式和递增式。这种原型法的成败及效率的高低,关键在于模型的建立及建模的速度。

2. 系统开发方法论

系统的开发方法主要包括结构化分析与设计、面向数据结构的设计、面向对象分析与设计以及构件化开发方法 4 种。

(1) 结构化分析与设计

这种方法采用结构化技术来完成软件开发的各项任务。该方法把软件生命周期的全过程依次划分为若干阶段,然后顺序地完成每个阶段的任务,与瀑布模型有很好的结合度,是与其最相适应的开发方法。

结构化方法的核心思想是“自顶向下,逐步分解”。

(2) 面向数据结构的设计

数据的输入、存储都涉及不同的数据结构,面向数据结构设计方法的基本思想是根据数据结构导出程序结构。典型的面向数据结构的设计方法包括 Jackson 方法和 Warnier 方法。

Jackson 方法的基本步骤是:先建立系统的数据结构;接着以数据结构为基础,对应地建立程序结构;列出程序中要用到的各种基本操作,然后将操作分配到适当的模块中。

面向数据结构的设计方法并没有明显地使用软件结构的概念,对于模块独立性原则也重视不足,因此并不适合于复杂的软件系统。

(3) 面向对象分析与设计

这种方法引入了“对象”的概念,将数据和方法封装在一起,提高了模块的聚合度,降低了耦合度,更大程度上支持软件复用。面向对象方法是目前非常流行和具有发展前景的软件开发方法。

面向对象分析是面向对象方法的核心之一,而且拥有大量不同的方法,主要包括 OMT、Coad/Yourdon 方法、OOSE 及 Booch 方法等,而 OMT、OOSE 及 Booch 最后统一称为统一建模语言(United Model Language, UML)。

① Coad/Yourdon 方法

Coad/Yourdon 方法由 P. Coad 和 E. Yourdon 于 1990 年推出,该方法主要由面向对象的分析(Object-Oriented Analysis, OOA)和面向对象的设计(Object-Oriented Design, OOD)构成,特别强调 OOA 和 OOD 采用完全一致的概念和表示法,使分析和设计之间不需要表示法的转换。该方法的特点是表示简练、易学,对于对象、结构、服务的认定较系统、完整,可操作性强。

在 Coad/Yourdon 方法中,OOA 的任务主要是建立问题域的分析模型。分析过程和构造 OOA 概念模型的顺序由 5 个层次组成,这 5 个层次是类与对象层、属性层、服务层、结构层和主题层,它们表示分析的不同侧面。OOA 需要经过 5 个步骤来完成整个分析工作,即

标识对象类、标识结构与关联（包括继承、聚合、组合、实例化等）、划分主题、定义属性和定义服务。

OOD 中将继续贯穿 OOA 中的 5 个层次和 5 个活动，它由 4 个部分组成，分别是人机交互部件、问题域部件、任务管理部件和数据管理部件，其主要的活动就是这 4 个部件的设计工作。

② Booch 方法

Booch 认为软件开发是一个螺旋上升的过程，每个周期包括 4 个步骤，分别是标识类和对象、确定类和对象的含义、标识关系、说明每个类的接口和实现。Booch 方法的开发模型包括静态模型和动态模型，静态模型分为逻辑模型（类图、对象图）和物理模型（模块图、进程图），描述了系统的构成和结构。动态模型包括状态图和时序图。该方法对每一步都做了详细的描述，描述手段丰富、灵活。不仅建立了开发方法，还提出了对设计人员的技术要求，不同开发阶段的人力资源配置。Booch 方法的基本模型包括类图与对象图，主张在分析和设计中既使用类图，也使用对象图。

③ OMT 方法

OMT（Object Model Technology，对象建模技术）作为一种软件工程方法学，它支持整个软件生存周期，覆盖了问题构成分析、设计和实现等阶段。OMT 方法使用了建模的思想，讨论如何建立一个实际的应用模型。从三个不同而又相关的角度建立了三类模型，分别是对象模型、动态模型和功能模型，OMT 为每一个模型提供了图形表示。

a. 对象模型。描述系统中对象的静态结构、对象之间的关系、属性、操作。它表示静态的、结构上的、系统的“数据”特征。主要用对象图来实现对象模型。

b. 动态模型。描述与时间和操作顺序有关的系统特征，如激发事件、事件序列、确定事件先后关系的状态。它表示瞬时、行为上的和系统的“控制”特征。主要用状态图来实现动态模型。

c. 功能模型。描述与值的变换有关的系统特征，包括功能、映射、约束和函数依赖。主要用数据流图来实现功能模型。

在进行 OMT 建模时，通常包括 4 个活动，分别是分析、系统设计、对象设计和实现。

a. 分析：建立可理解的现实世界模型。通常从问题陈述入手，通过与客户的不断交互以及对现实世界背景知识的了解，对能够反映系统的三个本质特征（对象类及它们之间的关系，动态的控制流，受约束的数据的函数变换）进行分析，构造出现实世界的模型。

b. 系统设计：确定整个系统的体系结构，形成求解问题和建立解答的高层策略。

c. 对象设计：在分析的基础上，建立基于分析模型的设计模型，并考虑实现细节。其焦点是实现每个类的数据结构及所需的算法。

d. 实现：将对象设计阶段开发的对象类及其关系转换为程序设计语言、数据库或硬件的实现。

④ OOSE

OOSE（Object-Oriented Software Engineering，面向对象的软件工程）在 OMT 的基础上，对功能模型进行了补充，提出了用例（use case）的概念，最终取代了数据流图进行需求分析和建立功能模型。

OOSE 方法采用 5 类模型来建立目标系统，这 5 类模型如下。

a. 需求模型：获取用户的需求，识别对象，主要的描述手段有用例图、问题域对象模

型及用户界面。

b. 分析模型：定义系统的基本结构。将分析模型中的对象分别识别到分析模型中的实体对象、界面对象和控制对象三类对象中。每类对象都有自己的任务、目标并模拟系统的某个方面。实体对象模拟那些在系统中需要长期保存并加以处理的信息，实体对象由使用事件确定，通常与现实生活中的一些概念相符合。界面对象的任务是提供用户与系统之间的双向通信，在使用事件中所指定的所有功能都直接依赖于系统环境，它们都放在界面对象中。控制对象的典型作用是将另外一些对象组合形成一个事件。

c. 设计模型：分析模型只注重系统的逻辑构造，而设计模型需要考虑具体的运行环境，将分析模型中的对象定义为模块。

d. 实现模型：用面向对象的语言来实现。

e. 测试模型：测试的重要依据是需求模型和分析模型，测试的方法与 4.5 节所介绍的类似，而底层是对类（对象）的测试。测试模型实际上是一个测试报告。

OOSE 的开发活动主要分为三类，分别是分析、构造和测试。其中分析过程分为需求分析和健壮分析两个子过程，分析活动分别产生需求模型和分析模型。构造活动包括设计和实现两个子过程，分别产生设计模型和实现模型。测试过程包括单元测试、集成测试和系统测试三个过程，共同产生测试模型。

用例是 OOSE 中的重要概念，在开发各种模型时，它是贯穿 OOSE 活动的核心，描述了系统的需求及功能。用例实际上是描述系统用户（使用者、执行者）对于系统的使用情况，是从使用者的角度来确定系统的功能。因此，首先必须分析确定系统的使用者，然后进一步考虑使用者的主要任务、使用的方式、识别所使用的事件，即用例。

（4）构件化开发

为了降低开发费用，提高生产率，以及在快速的技术演化面前提供受控的系统升级的开发方式，产生了基于构件的软件开发（Component-Based Software Development, CBSD）。

它通过有计划地集成现有的软件部分来进行软件开发。它可以有效地遏制复杂性，缩短发布时间，提高一致性，更有效地利用本领域的最佳方法，提高生产率，增加项目进度的可视性，支持并行和分布式的开发，减少维护费用。采用 CBSD 后，所有的软件解决方案将可以使用预建的构件和模板，像“搭积木”式地建造。

这种“积木”就是构件（组件），构件是一个功能相对独立的具有可重用价值的软件单元。在面向对象方法中，一个构件由一组对象构成，包含了一些协作的类的集合，它们共同工作来提供一种系统功能。

可重用性是指系统和（或）其组成部分能在其他系统中重复使用的程度。软件开发的全生命周期都有可重用的价值，包括项目的组织、软件需求、设计、文档、实现、测试方法和测试用例，都是可以被重复利用和借鉴的有效资源。可重用性体现在软件的各个层次，通用的、可复用性高的软件模块往往已经由操作系统或开发工具提供，如通用库、标准组件和标准模板库等，并不需要程序员重新开发。

3. 需求分析

本知识点的重点在于掌握需求分析的任务、过程、方法、原则，以及需求的详细分类与概念。

需求分析与设计是软件生存期中最重要的两个步骤，需求分析解决的是“做什么”的问题，系统设计解决的则是“怎么做”的问题。

(1) 需求分析的任务与过程

需求分析所要做的工作是深入地描述软件的功能和性能,确定软件设计的限制和软件同其他系统元素的接口细节,定义软件的其他有效性需求,细化软件要处理的数据域。需求分析的实现步骤通常包括:获取当前系统的物理模型,抽象出当前系统的逻辑模型,建立目标系统的逻辑模型三部分。具体来说,需求分析阶段的工作可以分成4个方面。

① 问题识别:用于发现需求、描述需求,主要包括功能需求、性能需求、环境需求、可靠性需求、安全保密需求、用户界面需求、资源使用需求、软件成本消耗与开发进度需求,以及预先估计以后系统可能达到的目标。

② 分析与综合:也就是对问题进行分析,然后在此基础上整合出解决方案。这个步骤经常是反复进行的,常用的方法有面向数据流的结构化分析方法(SA)、面向数据结构的 Jackson 方法、面向对象的分析方法(OOA),以及用于建立动态模型的状态迁移图和 Petri 网。

③ 编制需求分析的文档:也就是对已经确定的需求进行文档化描述,该文档通常称为“需求规格说明书”。

④ 需求分析与评审:它是需求分析工作的最后一步,主要对功能的正确性、完整性和清晰性,以及其他需求给予评价。

(2) 需求分析的原则

① 必须能够表达和理解问题的数据域和功能域。

② 必须按自顶向下、逐层分解的方式对问题进行分解和不断细化。

③ 要给出系统的逻辑视图和物理视图。

(3) 需求的分类

什么是软件的需求呢?软件需求就是系统必须完成的事,以及必须具备的品质。具体来说,软件需求包括功能需求、非功能需求和设计约束三方面内容,如图3-6所示。

a. 功能需求:是指系统必须完成的事情,即为了向它的用户提供有用的功能,产品必须执行的动作。

b. 非功能需求:是指产品必须具备的属性或品质,如可靠性、性能、响应时间、容错性、扩展性等。

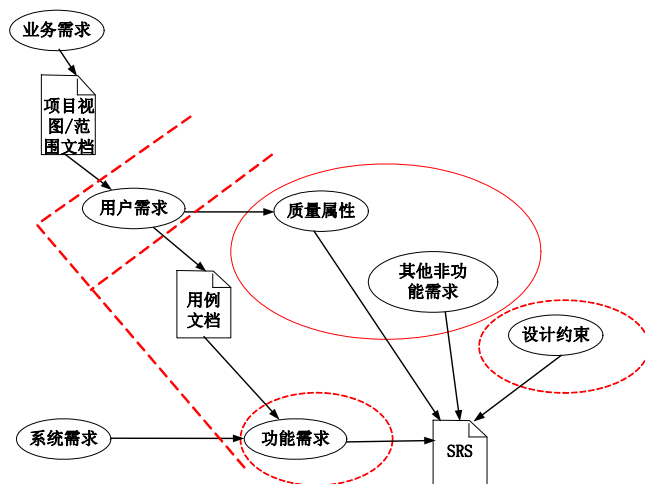


图 3-6 需求概念示意图

c. 设计约束：也称为限制条件、补充规约，这通常是对解决方案的一些约束说明，例如，必须采用国有自主知识产权的数据库系统，必须运行在 UNIX 操作系统下等。

除了这三种需求之外，还有业务需求、用户需求、系统需求这三个处于不同层面下的概念，充分理解这些模型才能够使你更加清晰地理清需求的脉络。

d. 业务需求 (Business Requirement)：是指反映组织机构或客户对系统、产品高层次的目标要求，通常问题定义本身就是业务需求。

e. 用户需求 (User Requirement)：是指描述用户使用产品必须完成什么任务，以及怎么完成需求，通常是在问题定义的基础上进行用户访谈、调查，对用户使用的场景进行整理，从而建立从用户角度出发的需求。

f. 系统需求 (System Requirement)：是从系统的角度来说明软件的需求，它包括用特性说明的功能需求、质量属性，以及其他非功能需求，还有设计约束。

我们经常围绕着“功能需求”来展开工作，而功能需求大都是从“系统需求”的角度来分析与理解的，也就是从“开发人员”的视角来理解需求。但要想真正地得到完整的需求，仅戴上“开发人员”的眼镜是不够的，我们还需要戴上“领域专家”的眼镜，从更高的角度来理解需求，这就是“业务需求”；同时我们还应该更好地深入用户，了解他们的使用场景，了解他们的所思所想，这就是“用户需求”。这是一个理解层次的问题，而不仅仅是简单的概念。

(4) 需求工程

需求工程就是包括创建和维护系统需求文档所必需的一切活动的过程，也就是指需求开发和需求管理两大工作。

a. 需求开发：包括需求捕获、需求分析、编写规格说明书和需求验证 4 个阶段。在这个阶段需要确定产品所期望的用户类型，获取每种用户类型的需求，了解实际用户任务和目标及这些任务所支持的业务需求，分析源于用户的信息，对需求进行优先级分类，将所收集的需求编写成为软件规格说明书和需求分析模型，对需求进行评审等工作。

b. 需求管理：通常包括定义需求基线、处理需求变更、需求跟踪等方面的工作。

这两个方面是相辅相成的，需求开发是主线，是目标；需求管理是支持，是保障。换句话说，需求开发是努力更清晰、明确地掌握客户对系统的需求，而需求管理则是对需求的变化进行管理的过程。

4. 软件设计

在软件设计阶段，主要考查结构化设计、模块内聚与耦合等概念。

(1) 软件设计阶段

从工程管理角度，软件设计可分为概要设计和详细设计两个阶段。

① 概要设计

概要设计也称为高层设计，将软件需求转化为数据结构和软件的系统结构。例如，如果采用结构化设计，则将从宏观的角度将软件划分成各个组成模块，并确定模块的功能以及模块之间的调用关系。

概要设计主要是设计软件的结构，确定系统是由哪些模块组成的，以及每个模块之间的关系。它采用的是结构图（包括模块、调用、数据）来描述程序的结构，还可以使用层次图和 HIPO（层次图加输入/处理/输出图）。整个过程主要包括：复查基本系统模型，复查并精化数据流图，确定数据流图的信息流类型（包括交换流和事务流），根据流类型分别实施变

换分析或事务分析，根据软件设计原则对得到的软件结构图进一步优化。

② 详细设计

详细设计也称为低层设计，将对结构表示进行细化，得到详细的数据结构与算法。同样，如果采用结构化设计，则详细设计的任务就是为每个模块进行设计。

详细设计确定应该如何具体地实现所要求的系统，得出对目标系统的精确描述。它采用自顶向下、逐步求精的设计方式和单入口单出口的控制结构。经常使用的工具包括程序流程图、盒图、PAD图（问题分析图）和PDL（伪码）。

总的来说，在整个软件设计过程中，需完成以下工作任务。

① 制定规范，作为设计的共同标准。

② 完成软件系统结构的总体设计，将复杂系统按功能划分为模块的层次结构，然后确定模块的功能，以及模块间的调用关系、模块间的组成关系。

③ 设计处理方式，包括算法、性能、周转时间、响应时间、吞吐量、精度等。

④ 设计数据结构。

⑤ 可靠性设计。

⑥ 编写设计文档，包括概要设计说明书、详细设计说明书、数据库设计说明书、用户手册、初步的测试计划等。

⑦ 设计评审，主要是对设计文档进行评审。

在设计阶段，必须根据要解决的问题，做出设计的选择。例如，对于半结构化决策问题就适合于交互式计算机软件来解决。

（2）软件设计活动

软件设计包括4个既独立又相互联系的活动：数据设计、体系结构设计、接口设计（界面设计）和过程设计。这4个活动完成以后就得到了全面的软件设计模型。设计方法也是以后实现设计模型的蓝图软件工程活动的基础。

数据设计是实施软件工程中4个设计活动的第一个。由于数据结构对程序结构和过程复杂性都有影响，因此数据结构对软件质量的影响是很深远的。好的数据设计将改善程序结构和模块划分，降低过程复杂性。数据设计将分析时创建的信息域模型变换成实现软件所需的数据结构。在实体-关系图（E-R图）中定义的数据对象和关系以及数据字典中描述的详细数据内容为数据设计活动奠定了基础。

体系结构设计的主要目标是开发一个模块化的程序结构，并表示出模块间的控制关系。此外，体系结构设计将程序结构和数据结构相结合，为数据在程序中的流动定义了接口。

接口设计描述了软件内部、软件和协作系统之间以及软件与人（用户）之间如何通信。一个接口意味着信息流（如数据和/或控制流），因此，数据和控制流图提供了接口设计所需的信息。接口设计要实现的内容包括一般交互、信息显示和数据输入。接口设计主要包括三个方面：

① 设计软件模块间的接口。

② 设计模块和其他非人的信息生产者和消费者（如外部实体）的接口。

③ 设计人（用户）和计算机间的接口（通常简称“人机接口”或“人机界面”）。

过程设计应该在数据设计、体系结构设计和接口设计完成之后进行。所有的程序都可以建立在一组已有的逻辑构成元素上，这一组逻辑构成元素强调了“对功能域的维护”，其中

每一个逻辑构成元素有可预测的逻辑结构，从顶端进入，从底端退出，读者可以很容易地理解过程流。

（3）结构化设计

结构化设计包括体系结构设计、接口设计、数据设计和过程设计等任务。它是一种面向数据流的设计方法，是以结构化分析阶段所产生的成果为基础，进一步自顶而下、逐步求精和模块化的过程。

在结构化方法中，模块化是一个很重要的概念，它是将一个待开发的软件分解成若干个小的简单部分（模块），每个模块可以独立地开发、测试。这是一种复杂问题的“分而治之”原则，其目的是使程序的结构清晰，易于测试与修改。

具体来说，模块是指执行某一特定任务的数据结构和程序代码。通常将模块的接口和功能定义为其外部特性，将模块的局部数据和实现该模块的程序代码称为内部特性。而在模块设计时，最重要的原则就是实现信息隐蔽和模块独立。模块通常具有连续性，也就是意味着作用于系统的小变动将导致行为上的小变化，同时规模说明的小变动也将影响到一小部分模块。

① 抽象化

对软件进行模块设计的时候，可以有不同的抽象层次。在最高的抽象层次上，可以使用问题所处环境的语言描述问题的解法。而在较低的抽象层次上，则采用过程化的方法。抽象化包括对过程的抽象、对数据的抽象和对控制的抽象。

a. 过程抽象。在软件工程过程中，从系统定义到实现，每进展一步都可以看作是对软件解决方案的抽象化过程的一次细化。在从概要设计到详细设计的过程中，抽象化的层次逐次降低，当产生源程序时到达最低的抽象层次。

b. 数据抽象。数据抽象与过程抽象一样，允许设计人员在不同层次上描述数据对象的细节。

c. 控制抽象。控制抽象可以包含一个程序控制机制而无须规定其内部细节。

② 自顶向下，逐步细化

将软件的体系结构按自顶向下方式，对各个层次的过程细节和数据细节逐层细化，直到用程序设计语言的语句能够实现为止，从而最后确立整个体系结构。最初的说明只是概念性地描述了系统的功能或信息，但并未提供有关功能的内部实现机制或有关信息的内部结构的任何信息。设计人员对初始说明仔细推敲，进行功能细化或信息细化，给出实现的细节，划分出若干成分。然后再对这些成分，施行同样的细化工作。随着细化工作的逐步展开，设计人员就能得到越来越多的细节。

③ 信息隐蔽

信息隐蔽是开发整体程序结构时使用的法则，即将每个程序的成分隐蔽或封装在一个单一的设计模块中，并且尽可能少地暴露其内部的处理。通常我们将难的决策、可能修改的决策、数据结构的内部连接，以及对它所做的操作细节、内部特征码、与计算机硬件有关的细节等隐蔽起来。

通过信息隐蔽可以提高软件的可修改性、可测试性和可移植性，它也是现代软件设计的一个关键性原则。

④ 模块独立

模块独立是指每个模块完成一个相对独立的特定子功能，并且与其他模块之间的联系最

简单。保持模块的高度独立性，也是设计时的一个很重要的原则。通常我们用耦合（模块之间联系的紧密程度）和内聚（模块内部各元素之间联系的紧密程度）两个标准来衡量，我们的目标是高内聚、低耦合。

模块的内聚类型通常可以分为 7 种，根据内聚度从高到低排序如表 3-1 所示。

表 3-1 模块的内聚类型

内聚类型	描述
功能内聚	完成一个单一功能，各个部分协同工作，缺一不可
顺序内聚	处理元素相关，而且必须顺序执行
通信内聚	所有处理元素集中在一个数据结构的区域上
过程内聚	处理元素相关，而且必须按特定的次序执行
瞬时应内聚	所包含的任务必须在同一时间间隔内执行（如初始化模块）
逻辑内聚	完成逻辑上相关的一组任务
偶然内聚	完成一组没有关系或松散关系的任务

与此相对应，模块的耦合类型通常也分为 7 种，根据耦合度从低到高排序如表 3-2 所示。

表 3-2 模块的耦合类型

耦合类型	描述
非直接耦合	没有直接联系，互相不依赖对方
数据耦合	借助参数表传递简单数据
标记耦合	一个数据结构的一部分借助于模块接口被传递
控制耦合	模块间传递的信息中包含用于控制模块内部逻辑的信息
外部耦合	与软件以外的环境有关
公共耦合	多个模块引用同一个全局数据区
内容耦合	一个模块访问另一个模块的内部数据；一个模块不通过正常入口转到另一模块的内部；两个模块有一部分程序代码重叠；一个模块有多个入口

除了满足以上两大基本原则之外，通常在模块分解时还应注意：保持模块的大小适中；尽可能减少调用的深度；直接调用该模块的个数应该尽量大，但调用其他模块的个数则不宜过大；保证模块是单入口、单出口的；模块的作用域应该在控制域之内；功能应该是可预测的。

5. 软件测试

在软件测试阶段，重点考查软件测试的目的、测试的类型、测试的阶段等知识点。

软件测试是软件质量保证的主要手段之一，也是在将软件交付给客户之前所必须完成的步骤。目前，软件的正确性证明尚未得到根本解决，软件测试仍是发现软件错误和缺陷的主要手段。软件测试的目的就是在软件投入生产性运行之前，尽可能多地发现软件产品（主要是指程序）中的错误和缺陷。

首先，测试并不仅仅是为了要找出错误。通过分析错误产生的原因和错误的分布特征，可以帮助项目管理者发现当前所采用的软件过程的缺陷，以便改进。同时，这种分析也能帮助我们设计出有针对性的检测方法，改善测试的有效性。

其次，没有发现错误的测试也是有价值的，完整的测试是评定测试质量的一种方法。

因此，软件测试可以验证软件是否满足软件需求规格说明和软件设计所规定的功能、性能及其软件质量特性的要求，为软件质量的评价提供依据。我们要注意的，软件测试只是

软件质量保证的手段之一，不能单凭测试来保证软件质量。

（1）测试的类型

软件测试方法一般分为两大类，即动态测试和静态测试。

① 动态测试

动态测试是指通过运行程序发现错误，分为黑盒测试法、白盒测试法和灰盒测试法。不管是哪一种测试，都不能做到穷尽测试，只能选取少量最有代表性的输入数据，期望用较低的代价暴露出较多的程序错误。这些被选取出来的数据就是测试用例（一个完整的测试用例应该包括输入数据和期望的输出结果）。

a. 黑盒法。把被测试对象看作一个黑盒子，测试人员完全不考虑程序的内部结构和处理过程，只在软件的接口处进行测试，依据需求规格说明书，检查程序是否满足功能要求。因此，黑盒测试又称为功能测试或数据驱动测试。常用的黑盒测试用例的设计方法有等价类划分、边值分析、错误猜测、因果图和功能图等。

b. 白盒法。把测试对象看作一个打开的盒子，测试人员需要了解程序的内部结构和处理过程，以检查处理过程的细节为基础，对程序中尽可能多的逻辑路径进行测试，检验内部控制结构和数据结构是否有错，实际的运行状态与预期的状态是否一致。由于白盒测试是结构测试，所以被测对象基本上是源程序，以程序的内部逻辑为基础设计测试用例。常用的白盒测试用例设计方法有基本路径测试、循环覆盖测试、逻辑覆盖测试。

c. 灰盒法。灰盒测试是一种介于白盒测试与黑盒测试之间的测试，它关注输出对于输入的正确性。同时也关注内部表现，但这种关注不像白盒测试那样详细且完整，而只是通过一些表征性的现象、事件及标志来判断程序内部的运行状态。

② 静态测试

静态测试是指被测试程序不在机器上运行，而是采用人工检测和计算机辅助静态分析的手段对程序进行检测。静态分析中进行人工测试的主要方法有桌前检查（Desk Checking）、代码审查和代码走查。经验表明，使用这种方法能够有效地发现 30%~70% 的逻辑设计和编码错误。

值得说明的是，使用静态测试的方法也可以实现白盒测试。例如，使用人工检查代码的方法来检查代码的逻辑问题，也属于白盒测试范畴。

（2）测试的阶段

为了保证系统的质量和可靠性，应力求在分析、设计等各个开发阶段结束前，对软件进行严格的技术评审。而软件测试是为了发现错误而执行程序的过程。

根据测试的目的、阶段的不同，可以把测试分为单元测试、集成测试、确认测试、系统测试等种类。

① 单元测试

单元测试又称为模块测试，是针对软件设计的最小单位（程序模块）进行正确性检验的测试工作。其目的在于检查每个程序单元能否正确实现详细设计说明中的模块功能、性能、接口和设计约束等要求，发现各模块内部可能存在的各种错误。单元测试需要从程序的内部结构出发设计测试用例，多个模块可以平行地独立进行单元测试。

单元测试根据详细设计说明书，包括模块接口测试、局部数据结构测试、路径测试、错误处理测试和边界测试，单元测试通常由开发人员自己负责。而由于通常程序模块不是单独存在的，因此常常要借助驱动模块（相当于用于测试模拟的主程序）和桩模块（子模块）完

成。单元测试的计划通常是在软件详细设计阶段完成。

② 集成测试

集成测试也称为组装测试、联合测试（对于子系统而言，则称为部件测试）。它主要是将已通过单元测试的模块集成在一起，主要测试模块之间的协作性。集成测试计划通常是在软件概要设计阶段完成。

从组装策略而言，可以分为一次性组装和增量式组装，增量式组装又包括自顶向下、自底向上、混合式三种，其中混合式组装又称为三明治式测试。

a. 自顶向下集成测试：是一种构造程序结构的增量实现方法。模块集成的顺序是首先集成主控模块（主程序），然后按照控制层次结构向下进行集成。隶属于（和间接隶属于）主控模块的模块按照深度优先或者广度优先的方式集成到整个结构中。

b. 自底向上集成测试：是从原子模块（例如在程序结构的最底层的模块）开始来进行构造和测试的，与自顶向下集成测试相反。

c. 三明治式测试：是一种组合的折中测试策略，从“两头”往“中间”测试，其在程序结构的高层使用自顶向下策略，而在下面的较低层中使用自底向上策略，类似于“两片面包间夹馅的三明治”而得名。

软件集成的过程是一个持续的过程，会形成多个临时版本。在不断的集成过程中，功能集成的稳定性是真正的挑战。在每个版本提交时，都需要进行冒烟测试，即对程序主要功能进行验证。冒烟测试也称为版本验证测试或提交测试。

③ 确认测试

确认测试也称为有效性测试，主要是验证软件的功能、性能及其他特性是否与用户要求（需求）一致。确认测试计划通常是在需求分析阶段完成的。根据用户的参与程度，通常包括下面 4 种类型。

a. 内部确认测试：主要由软件开发组织内部按软件需求说明书进行测试。

b. α 测试（Alpha 测试）：由用户在开发环境下进行测试。

c. β 测试（Beta 测试）：由用户在实际使用环境下进行测试。

d. 验收测试：针对软件需求说明书，在交付前以用户为主进行的测试。

④ 系统测试

如果项目不仅包含软件，还有硬件和网络等，则要将软件与外部支持的硬件、外设、支持软件、数据等其他系统元素结合在一起，在实际运行环境下，对计算机系统的一系列集成与确认测试。一般系统测试的主要内容包括功能测试、健壮性测试、性能测试、用户界面测试、安全性测试、安装与反安装测试等。系统测试计划通常是在系统分析阶段（需求分析阶段）完成的。

不管是哪个阶段的测试，一旦测试出问题，就要进行修改。修改之后，为了检查这种修改是否会引起其他错误，还要对这个问题进行测试，这种测试称为回归测试或退化测试。

（3）性能测试

性能测试是通过自动化的测试工具模拟多种正常、峰值以及异常负载条件来对系统的各项性能指标进行测试。负载测试和压力测试都属于性能测试，两者可以结合进行。通过负载测试，确定在各种工作负载下系统的性能，目标是测试当负载逐渐增加时，系统各项性能指标的变化情况。压力测试是通过确定一个系统的瓶颈或者不能接收的性能点，来获得系统能

提供的最大服务级别的测试。

① 性能测试的目的

性能测试的目的是验证软件系统是否能够达到用户提出的性能指标，同时发现软件系统中存在的性能瓶颈，优化软件，最后起到优化系统的目的。

② 性能测试的类型

性能测试类型包括负载测试、强度测试和容量测试等。

- a. 负载测试：是一种性能测试，是指数据在超负荷环境中运行，程序是否能够承担。
- b. 强度测试：是一种性能测试，它在系统资源特别少的情况下测试软件系统运行情况。
- c. 容量测试：确定系统可处理的同时在线的最大用户数。

③ 负载压力测试

系统的负载压力测试（负载测试）是指系统在某种指定软件、硬件及网络环境下承受的流量，例如并发用户数、持续运行时间、数据量等，其中并发用户数是负载压力的重要体现。系统在应用环境下主要承受并发访问用户数、无故障稳定运行时间、大数据量操作等负载压力。

负载压力测试的目的如下：

- a. 在真实环境下检测系统性能，评估系统性能是否可以满足系统的性能设计要求。
- b. 预见系统负载压力承受力，对系统的预期性能进行评估。
- c. 进行系统瓶颈分析、优化系统。

(4) 第三方测试

第三方测试指独立于软件开发方和用户方的测试，组织的测试也称为“独立测试”。软件质量工程强调开展独立验证和确认（IV&V）活动，是由在技术、管理和财务上与开发组织具有规定程序独立的组织执行验证和确认过程。软件第三方测试也指相对独立的组织进行的软件测试，一般情况下是在模拟用户真实应用环境下，进行软件确认测试。

第三方测试机构是一个中介的服务机构，它通过自己专业化的测试手段为客户提供有价值的服务。但是这些服务不同于公司内部测试，因为第三方测试机构的测试除了发现软件问题之外，还有科学公正地评价软件的职能，这就要求该机构要保持公正、廉洁、客观、科学且独立的态度。

第三方测试机构存在的价值主要是由软件公司、软件用户，以及国家的公正诉求所决定的。对于软件开发商来说，经过第三方测试机构的测试，不仅可以通过专业化的测试手段发现软件错误，帮助开发商提升软件的品质；而且可以对软件有一个客观且科学的评价，有助于开发商认清自己产品的定位。对于行业主管部门以及软件使用者来说，第三方测试机构可帮助选择合适且优秀的软件产品。而对于一些信息工程项目来说，在验收之前，经过第三方机构的严格测试，可以最大程度地避免信息行业的“豆腐渣”工程。此外，经过国家认可的第三方测试机构，还为国家软件产品的质量监督检查提供独立公正的测试支持。

在选择第三方测试机构时，主要查看其资质、信息系统工程测评经验、测试环境、测试工具及测试工程师队伍的素质等。

3.2.2 一点一练

试题 1

下列叙述中，与提高软件可移植性相关的是__（1）__。

- (1) A. 选择时间效率高的算法

- B. 尽可能减少注释
- C. 选择空间效率高的算法
- D. 尽量用高级语言编写系统中对效率要求不高的部分

试题 2

在开发一个系统时，如果用户对系统的目标不是很清楚，难以定义需求，这时最好使用____(2)_____。

- (2) A. 原型法 B. 瀑布模型 C. V 模型 D. 螺旋模型

试题 3

应该在____(3)_____阶段制订系统测试计划。

- (3) A. 需求分析 B. 概要设计 C. 详细设计 D. 系统测试

试题 4

软件设计时需要遵循抽象、模块化、信息隐蔽和模块独立原则，在划分软件系统模块时，应尽量做到____(4)_____。

- (4) A. 高内聚高耦合 B. 高内聚低耦合
C. 低内聚高耦合 D. 低内聚低耦合

试题 5

渐增式开发方法有利于____(5)_____。

- (5) A. 获取软件需求 B. 快速开发软件
C. 大型团队开发 D. 商业软件开发

试题 6

基于计算机的信息系统主要包括计算机硬件系统、计算机软件系统、数据及其存储介质、通信系统、信息采集设备、____(6)_____和工作人员等 7 大部分。

- (6) A. 信息处理系统 B. 信息管理者
C. 安全系统 D. 规章制度

试题 7

____(7)_____是面向对象程序设计语言不同于其他语言的主要特点，是否建立了丰富的____(8)_____是衡量一个面向对象程序设计语言成熟与否的重要标志之一。

- (7) A. 继承性 B. 信息传递 C. 多态性 D. 静态联编
(8) A. 函数库 B. 类库 C. 类型库 D. 方法库

试题 8

在面向对象的软件工程中，一个组件包含了____(9)_____。

- (9) A. 所有的属性和操作 B. 各个类的实例
C. 每个演员 (device or user) 的作用 D. 一些协作类的集合

试题 9

常见的软件开发模型有瀑布模型、演化模型、螺旋模型、喷泉模型等。其中____(10)_____模型适用于需求明确或很少变更的项目。

- (10) A. 瀑布模型 B. 演化模型 C. 螺旋模型 D. 喷泉模型

试题 10

一个项目为了修正一个错误而进行了变更，这个错误被修正后却引起了____(11)_____。

- (11) A. 单元测试 B. 接受测试 C. 回归测试 D. 安装测试

3.2.3 解析与答案

试题 1 分析

软件可移植性指与软件从某一环境转移到另一环境下的难易程度。为获得较高的可移植性，在设计过程中常采用通用的程序设计语言和运行支撑环境。尽量不用与系统的底层相关性强的语言。

试题 1 答案

(1) D

试题 2 分析

应用原型法的主要目的就是获取需求，使用原型法，在用户的共同参与下可以改善和加快需求获取过程。

试题 2 答案

(2) A

试题 3 分析

软件测试是一个长时间的过程，其测试计划的制订应该是尽可能早，一般在需求分析阶段就开始制订测试计划。

试题 3 答案

(3) A

试题 4 分析

内聚性能是指一个软件模块内部相关性。而耦合性能指不同软件模块之间的相关性或者依赖性。高内聚指一个软件模块由相关性很强的代码组成，只负责完成一项任务，即单一责任原则；低耦合指不同软件模块之间通过稳定的接口交互，而不需要关心模块内部如何实现。高内聚和低耦合是相互矛盾的，分解粒度越粗的系统耦合性越低；分解粒度越细的系统内聚性越高。过度低耦合的软件系统模块内部不可能高内聚，而过度高内聚的软件模块之间必然是高度依赖的，因此软件设计时尽量做到高内聚、低耦合。

试题 4 答案

(4) B

试题 5 分析

增量模型又称渐增模型，把软件产品作为一系列的增量构件来设计、编码、集成和测试。这样可以并行开发构件，快速开发软件。

试题 5 答案

(5) B

试题 6 分析

信息系统主要包括计算机硬件系统、计算机软件系统、数据及其存储介质、通信系统、信息采集设备、规章制度和工作人员等 7 大部分。

试题 6 答案

(6) D

试题 7 分析

面向对象程序设计语言的特点主要有继承性、封装性和多态性，其中，继承性是其他类型的程序语言所不具有的。衡量一个面向对象程序设计语言成熟与否的重要标志之一是看其

是否建立了丰富的类库。

试题 7 答案

(7) A

(8) B

试题 8 分析

在面向对象的软件工程中，一个组件（component）包含了一些协作的类的集合。这属于常识知识。

试题 8 答案

(9) D

试题 9 分析

本题考查的是常见的软件开发模型的基本概念。

瀑布模型给出了软件生存周期中制订开发计划、需求分析、软件设计、编码、测试和维护等阶段以及各阶段的固定顺序，上一阶段完成后才能进入下一阶段，整个过程如同瀑布流水。该模型为软件的开发和维护提供了一种有效的管理模式，但在大量的实践中暴露出其缺点，其中最为突出的是缺乏灵活性，特别是无法解决软件需求不明确或不准确的问题。这些问题有可能造成开发出的软件并不是用户真正需要的，并且这一点只有在开发过程完成后才能发现。所以瀑布模型适用于需求明确且很少发生较大变化的项目。

试题 9 答案

(10) A

试题 10 分析

本题考查软件测试的基本概念，这里的回归测试是在软件发生变更之后进行的测试，以发现在变更时可能引起的其他错误。

试题 10 答案

(11) C

3.3 项目管理

在软件项目管理方面，主要涉及软件项目估算、进度计划与监控、质量管理、软件过程改进 4 方面的内容。

3.3.1 考点精讲

软件项目估算是给定公差范围内，对于要开发的软件规模的预测，以及对开发软件所需的工作量、成本和日历事件的预测，也就是估算是一种大约的估计，是将误差限定在一定范围内的估计。进度计划与监控对于一个项目能否如期完成非常重要。软件质量管理是为了保证软件系统或软件产品充分满足用户所要求的质量。软件过程改进涉及软件过程能力成熟度模型（Capability Maturity Model, CMM）和能力成熟度模型集成（Capability Maturity Model Integration, CMMI）两个模型。

1. 软件项目估算

项目估算的内容包括软件规模估算、软件工作量估算与成本估算三个方面。

(1) 估算策略

估算策略包括“自顶向下”和“自底向上”两种。

① 自顶向下：以项目经理为核心，先根据用户、决策者的要求，确定一个时间期限，

然后根据该期限进行分解,采用对号入座的方式将开发工作分配给具体的开发人员,以获得一个可以满足这个期限的估算。

② 自底向上:由核心小组进行头脑风暴,完成工作任务分解,然后由开发人员进行合理估算,再累计得到总的估算。

(2) 估算规模估算

也就是估算要完成的工作范围,常用的方法有 LOC 估算法和 FP 估算法。

① LOC 估算法:代码行估算法,将项目切分为一个个小模块,通过历史项目经验、开发人员经验,估算每个模块的代码行。

② FP 估算法:FP 是指功能点,是一种衡量工作量大小的单位。它的计算方法是,功能点=信息处理规模 \times 技术复杂度。其中,技术复杂度=0.65+调节因子。它首先通过外部输入数(input)、外部输出数(output)、外部查询数(inquire)、内部逻辑文件数(file)、外部接口文件数(interface)5个方面来衡量整个系统的信息处理规模(根据难度乘上系数,难度级别分为低、平均、高三级),然后再从数据通信、分布式处理、性能、配置项、事务率、在线数据、用户使用效率、在线更新、复杂处理、重用性、安装容易程度、操作容易程度、多个地点、修改容易程度14个方面的复杂度,进行微调,每个方面都在0~0.05之间取值,最后累加出调节因子,再加上0.65得出技术复杂度。

(3) 软件工作量估算

工作量的单位通常是人月,计算方法为:规模/产能=工作量。

① IBM 模型:是在60多个项目的基础上进行统计得出的静态模型。

② Putnum 模型:是一种动态多变量模型,它通过建立一个“资源需求曲线模型”来导出一系列等式,模型化资源特性。

③ COCOMO 模型:是最有代表性的方法。在该模型中使用了源指令条数(DSI)、开发工作量(MM)、开发进度(TDEV)三个基本量,它将项目分为组织型(相对较小、较简单的项目)、嵌入式(软、硬件限制较多的项目)、半独立型(介于两者之间,规模和复杂性中等以上)。它包括基本(静态模型)、中间、详细三种不同的模型。

(4) 成本估算

得到工作量、人员需求、项目持续时间后,就可以进一步估算成本,通常包括人员成本、资源成本、其他开支等。

2. 进度计划与监控

项目的进度安排与任何一个多重任务工作的进度安排基本类似。项目的进度计划和工作的实际进展情况,通常表现为各项任务之间的进度依赖关系,因而通常使用图表的方式来原因。

(1) 甘特图

甘特图(Gantt 图)使用水平线段表示任务的工作阶段,线段的起点和终点分别对应着任务的开工时间和完成时间,线段的长度表示完成任务所需的时间。而跟踪甘特图则是在甘特图的基础上,加上一个表示现在时间的纵线,可以直观地看出进度是否延误。甘特图的优点在于标明了各任务的计划进度和当前进度,能动态地反映项目进展;其缺点在于难以反映多个任务之间存在的复杂逻辑关系。

(2) PERT 技术和 CPM 方法

PERT（计划评审技术）和 CPM（关键路径法）都是采用网络图来描述一个项目的任务网络，通常使用两张图来定义网络图。一张图给出某一特定项目的所有任务，另一张图给出应按照什么次序来完成这些任务，给出各个任务之间的衔接。PERT 技术和 CPM 方法都为项目计划人员提供了一些定量的工具。

- ① 确定关键路径：即决定项目开发时间的任务链。
- ② 应用统计模型：对每个单独的任务确定最可能的持续时间的估算值。
- ③ 计算边界时间：为具体的任务定义时间窗口。

CPM 是借助网络图和各活动所需的时间（估计值），计算每一活动的最早或最迟开始和结束时间。CPM 方法的关键是计算总时差，这样可决定哪一个活动有最小时间弹性。CPM 方法的核心思想是将 WBS 分解的活动按逻辑关系加以整合，统筹计算出整个项目的工期和关键路径。

在网络图中的某些活动可以并行地进行，所以完成工程的最少时间是从开始顶点到结束顶点的最长路径长度，称从开始顶点到结束顶点的最长（工作时间之和最大）路径为关键路径（临界路径），关键路径上的活动为关键活动。在一条路径中，每个工作的时间之和等于工程工期，这条路径就是关键路径。

例如，在图 3-7 中，一共有 3 条路径，分别是 ABEG、ACFG 和 ABDFG，其路径长度分别为 16、17 和 21。因此，图 3-7 的关键路径为 ABDFG。如果图 3-7 是代表某个项目的网络计划图，则该项目的工期为 21 天。

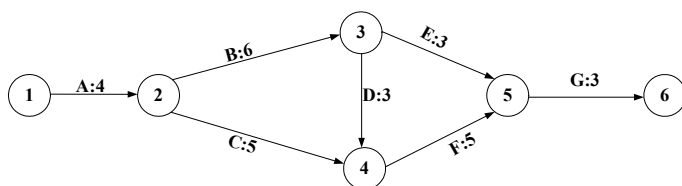


图 3-7 某项目的网络计划图

又如，某网络工程的计划图如图 3-8 所示。

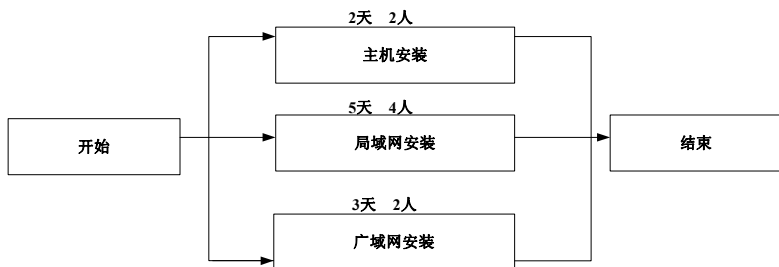


图 3-8 某网络工程的计划图

在图 3-8 中，一共有 3 条路径，分别是①开始→主机安装→结束；②开始→局域网络安装→结束；③开始→广域网络安装→结束。从图中可知，这 3 条路径可以并行执行，因此，项目的最短工期为 5 天。如果每个技术人员均能胜任每项工作，则至少需要投入 6 人才能完成该项目。因为主机安装只需要 2 天 2 人，而广域网络安装也只需要 3 天 2 人，因此，这两项工作采用安排 2 人顺序执行的方式。例如，前 2 天从事主机安装，后 3 天从事广域网络安装，这样，合计为 5 天，不会影响整个项目的工期。

（3）评估项目进度

最常见的方法是挣值分析，它是把实际进度和计划进度进行比较，发现项目是否拖期或超前。通过计算实际已花费在项目上的工作量，来预计该项目所需的成本和完成时间日期。

3. 质量管理

软件质量是软件特性的综合，是指软件满足规定或潜在用户需求的能力。具体地说，软件质量是软件与明确叙述的功能和性能需求、文档中明确描述的开发标准，以及任何专业开发的软件产品都应该具有的隐含特征相一致的程度。

软件质量保证是指为保证软件系统或软件产品充分满足用户要求的质量而进行的有计划、有组织的活动，这些活动贯穿于软件生产的各个阶段，即整个生命周期。

影响软件质量的因素主要包括：人、软件需求、开发过程的各个环节、测试的局限性、质量管理的困难性、是否对质量管理予以重视、软件人员的传统习惯、开发规范和支持性的开发工具等方面。

为了能够统一地描述软件质量特性，形成了许多质量特性标准，其中最常用的有国际通用的 ISO/IEC 9126 软件质量模型和 McCall 软件质量模型。

（1）ISO/IEC 9126 模型

该标准已于 1996 年被采纳为我国的国家标准《GB/T 16120-1996 软件产品评价、质量特性及其使用指南》，其包括 6 类 21 个质量特性，如表 3-3 所示。

表 3-3 GB/T 16120-1996 软件产品评价、质量特性及其使用指南

质 量 属 性	子 特 性	说 明
功能性	与功能及其指定的性质有关的一组软件质量	
	适合性	规定任务提供一组功能的能力，以及这组功能的适合程度
	准确性	系统满足需求规格说明和用户目标的程度
	互操作性	同其他指定系统的协同工作能力
	依从性	软件服从有关标准、约定、法规及类似规定的程度
	安全性	避免对程序及数据的非授权故意或意外访问的能力
可靠性	衡量在规定的时间内和规定条件下维护性能水平的一组软件质量	
	成熟性	由软件故障引起失效的频度
	容错性	在错误或违反指定接口情况下维护指定性能水平的能力
	易恢复性	在故障发生后重新建立性能水平，恢复数据的能力和恢复时间
易使用性	与使用难易程度及规定或隐含用户对使用方式所做的评价相关的属性	
	易理解性	用户理解该软件系统的难易程度
	易学习性	用户学习使用该软件系统的难易程度
	易操作性	用户操作该软件系统的难易程度
效率	衡量在规定条件下软件的性能水平和所用资源量之间的关系的属性	
	时间特性	响应和处理时间及软件执行其功能时的吞吐量
	资源特性	软件执行其功能时，所使用的资源量及持续使用时间
可维护性	与软件维护的难易程度相关的一组软件属性	
	易分析性	诊断缺陷或失效原因，判定待修改程度的难易程度
	易更改性	修改、排错或适应环境变化的难易程度
	稳定性	修改造成难以预料的后果的风险程度
	易测试性	测试已修改软件的难易程度

续表

质量属性	子特性	说明
可移植性	与从某一环境转移到另一环境的能力有关的属性	
	适应性	软件无须采用特殊处理就能够适应不同规定环境的程度
	易安装性	在指定环境下安装软件的难易程度
	一致性	软件服从与可移植性有关的标准或约束的程度
	易替换性	软件在特定软件环境中用来替代指定的其他软件的可能性和难易程度

(2) McCall 质量模型

McCall 质量模型体系如表 3-4 所示。

表 3-4 McCall 质量模型体系

类别	质量特性	含义
运行	正确性	程序能够满足规格说明和完成用户业务目标的程度
	可靠性	程序能够按要求的精确度实现其预期功能的程度
	效率	程序实现其功能所需要的计算资源量
	完整性	软件或数据不受未授权人控制的程度
	使用性	学习、操作程序、为其准备输入数据、解释其输出的工作量
修正	维护性	对运行的程序找到错误并排错的工作量
	测试性	为保证程序执行规定功能所需的测试工作量
	灵活性	修改运行的程序所需的工作量
转移	移植性	将程序从一种硬件配置和/或环境转移到另一硬件配置和/或环境所需的工作量
	复用性	程序可被用于与其实现功能相关的其他应用问题的程度
	共运行性	让系统与另一系统协同运行所需的工作量

4. 软件过程改进

在软件过程改进方面，主要考查软件过程能力成熟度模型（Capability Maturity Model, CMM）和能力成熟度模型集成（Capability Maturity Model Integration, CMMI）。

(1) CMM

CMM 模型描述和分析了软件过程能力的发展程度，确立了一个软件过程成熟程度的分级标准。

① 初始级：软件过程的特点是无秩序的，有时甚至是混乱的。软件过程定义几乎处于无章法和步骤可循的状态，软件产品所取得的成功往往依赖极个别人的努力和机遇。初始级的软件过程是未加定义的随意过程，项目的执行是随意甚至是混乱的。也许，有些企业制定了一些软件工程规范，但若这些规范未能覆盖基本的关键过程要求，且执行没有政策、资源等方面的保证时，那么它仍然被视为初始级。

② 可重复级：已经建立了基本的项目管理过程，可用于对成本、进度和功能特性进行跟踪。对类似的应用项目，有章可循并能重复以往所取得的成功。焦点集中在软件管理过程上。一个可管理的过程则是一个可重复的过程，一个可重复的过程则能逐渐演化和成熟。从管理角度可以看到一个按计划执行的且阶段可控的软件开发过程。

③ 已定义级：用于管理的和工程的软件过程均已文档化、标准化，并形成整个软件组织的标准软件过程。全部项目均采用与实际情况相吻合的、适当修改后的标准软件过程来进行操作。要求制定企业范围的工程化标准，而且无论是管理还是工程开发都需要一套文档化

的标准，并将这些标准集成到企业软件开发标准过程中去。所有开发的项目需根据这个标准过程，剪裁出项目适宜的过程，并执行这些过程。过程的剪裁不是随意的，在使用前需经过企业有关人员的批准。

④ 已管理级：软件过程和产品质量有详细的度量标准。软件过程和产品质量得到了量的认识和控制。已管理级的管理是量化的管理。所有过程需建立相应的度量方式，所有产品的质量（包括工作产品和提交给用户的产品）需有明确的度量指标。这些度量应是详尽的，且可用于理解和控制软件过程和产品，量化控制将使软件开发真正变成一个工业生产活动。

⑤ 优化级：通过对来自过程、新概念和新技术等方面的各种有用信息的定量分析，能够不断地、持续地进行过程改进。如果一个企业达到了这一级，表明该企业能够根据实际的项目性质、技术等因素，不断调整软件生产过程以求达到最佳。

在 CMM 中，每个成熟度等级（第一级除外）规定了不同的关键过程域，一个软件组织如果希望达到某一个成熟度级别，就必须完全满足关键过程域所规定的要求，即满足关键过程域的目标。每个级别对应的关键过程域（KPA）见表 3-5。

表 3-5 关键过程域的分类

过程分类 等 级	管 理 方 面	组 织 方 面	工 程 方 面
优化级		技术改进管理 过程改进管理	缺陷预防
可管理级	定量管理过程		软件质量管理
已定义级	集成（综合）软件管理 组间协调	组织过程焦点 组织过程定义 培训程序	软件产品工程 同级评审
可重复级	需求管理 软件项目计划 软件项目跟踪与监控 软件子合同管理 软件质量保证 软件配置管理		

(2) CMMI

与 CMM 相比，CMMI 涉及面更广，专业领域覆盖软件工程、系统工程、集成产品开发和系统采购。据美国国防部资料显示，运用 CMMI 模型管理的项目，不仅降低了项目的成本，而且提高了项目的质量与按期完成率。

CMMI 可以看作是各种 CMM 集成到一个系列的模型中，CMMI 的基础源模型包括软件 CMM 2.0 版（草稿 C）、EIA-731 系统工程，以及集成化产品和过程开发 IPD CMM（IPD）0.98a 版。CMMI 也描述了 5 个不同的成熟度级别。

每一种 CMMI 模型都有两种表示法：阶段式和连续式。这是因为在 CMMI 的三个源模型中，CMM 是“阶段式”模型，系统工程能力模型是“连续式”模型，而集成产品开发（IPD）CMM 是一个混合模型，组合了阶段式和连续式两者的特点。两种表示法在以前的使用中各有优势，都有很多支持者，因此，CMMI 产品开发群组在集成这三种模型时，为了避免由于淘汰其中任何一种表示法而失去对 CMMI 支持的风险，并没有选择单一的结构表示法，而是为每一个 CMMI 都推出了两种不同表示法的版本。

不同表示法的模型具有不同的结构。连续式表示法强调的是单个过程域的能力，从过程域的角度考察基线和度量结果的改善，其关键术语是“能力”；而阶段式表示法强调的是组织的成熟度，从过程域集合的角度考察整个组织的过程成熟度阶段，其关键术语是“成熟度”。

尽管两种表示法的模型在结构上有所不同，但 CMMI 产品开发群组仍然尽最大努力确保了两者在逻辑上的一致性，二者的需要构件和期望部件基本上都是一样的。过程域、目标在两种表示法中都一样，特定实践和共性实践在两种表示法中也不存在根本区别。因此，模型的两种表示法并不存在本质上的不同。组织在进行集成化过程改进时，可以从实用角度出发选择某一种偏爱的表示法，而不必从哲学角度考虑两种表示法之间的差异。

阶段式模型也把组织分为 5 个不同的级别。

① 初始级：代表了以不可预测结果为特征的过程成熟度，过程处于无序状态，成功主要取决于团队的技能。

② 已管理级：代表了以可重复项目执行为特征的过程成熟度。组织使用基本纪律进行需求管理、项目计划、项目监督和控制、供应商协议管理、产品和过程质量保证、配置管理，以及度量和分析。对于级别 2 而言，主要的过程焦点在于项目级的活动和实践。

③ 严格定义级：代表了以组织内改进项目执行为特征的过程成熟度。强调级别 3 的关键过程域的前后一致的、项目级的纪律，以建立组织级的活动和实践。

④ 定量管理级：代表了以改进组织性能为特征的过程成熟度。4 级项目的历史结果可用来交替使用，在业务表现的竞争尺度（成本、质量、时间）方面的结果是可预测的。

⑤ 优化级：代表了以可快速进行重新配置的组织性能和定量的、持续的过程改进为特征的过程成熟度。

CMMI 的具体目标是：

① 改进组织的过程，提高对产品开发和维护的管理能力。

② 给出能支持将来集成其他科目 CMM 的公共框架。

③ 确保所开发的全部有关产品符合将要发布的关于软件过程改进的国际标准 ISO/IEC 15504 对软件过程评估的要求。

使用在 CMMI 框架内开发的模型具有下列优点：

① 过程改进能扩展到整个企业级。

② 先前各模型之间的不一致和矛盾将得到解决。

③ 既有分级的模型表示，也有连续的模型表示，任你选用。

④ 原先单科目过程改进的工作可与其他科目的过程改进工作结合起来。

⑤ 基于 CMMI 的评估将与组织原先评估得分相协调，从而保护当前的投资，并与 ISO/IEC 15504 评估结果相一致。

⑥ 节省费用，特别是当要运用多科目改进时，以及进行相关的培训和评估时。

⑦ 鼓励组织内各科目之间进行沟通和交流。

3.3.2 一点一练

试题 1

使用 LOC (Lines of Code) 度量软件规模的优点是 (1)。

(1) A. 容易计算

B. 与使用的编程语言有关

C. 与采用的开发模型有关

D. 在设计之前就可以计算出 LOC

试题 2

在软件项目管理中可以使用各种图形工具来辅助决策,下面对 Gantt 图的描述中,不正确的是____(2)_____。

- (2) A. Gantt 图表现了各个活动的持续时间
B. Gantt 图表现了各个活动的起始时间
C. Gantt 图反映了各个活动之间的依赖关系
D. Gantt 图表现了完成各个活动的进度

试题 3

CMM 模型将软件过程的成熟度分为 5 个等级,在____(3)_____使用定量分析来不断地改进和管理软件过程。

- (3) A. 优化级 B. 管理级 C. 定义级 D. 可重复级

试题 4

某网络工程计划图如图 3-9 所示,边上的标记为任务编码及其需要的完成时间(天),则整个工程的工期为____(4)_____。

- (4) A. 23 B. 10 C. 17 D. 21

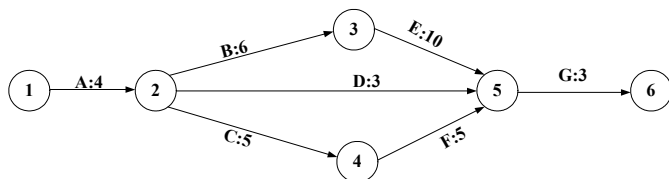


图 3-9 某项目的网络计划图

试题 5

ISO/IEC 9126 软件质量模型中第一层定义了 6 个质量特性,并为各质量特性定义了相应的质量子特性。子特性____(5)_____属于可靠性质量特性。

- (5) A. 准确性 B. 易理解性 C. 成熟性 D. 易学性

试题 6

若一个项目由 9 个主要任务构成,其计划图(如图 3-10 所示)展示了任务之间的前后关系以及每个任务所需天数,该项目的关键路径是____(6)_____。

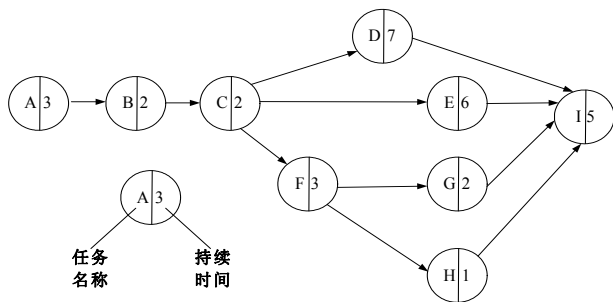


图 3-10 某项目的网络计划图

- (6) A. A→B→C→D→I B. A→B→C→E→I
C. A→B→C→F→G→I D. A→B→C→F→H→I

试题 7

软件能力成熟度模型（CMM）将软件能力成熟度自低到高依次划分为初始级、可重复级、定义级、管理级和优化级，其中（7）对软件过程和产品都有定量的理解与控制。

- (7) A. 可重复级和定义级 B. 定义级和管理级
C. 管理级和优化级 D. 定义级、管理级和优化级

试题 8

确定构建软件系统所需要的人数时不必考虑（8）。

- (8) A. 系统的市场前景 B. 系统的规模
C. 系统的技术复杂性 D. 项目计划

试题 9

如图所示的 PERT 图 3-11 中，事件 6 的最晚开始时刻是（9）。

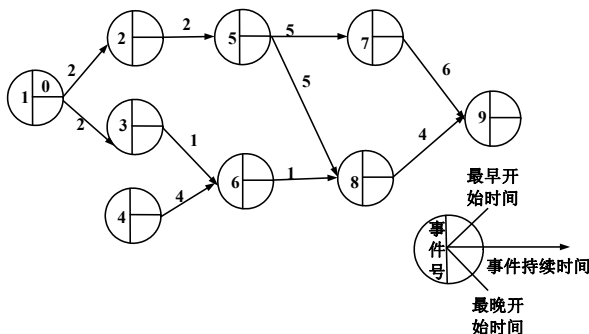


图 3-11 某项目的网络计划图

- (9) A. 0 B. 3 C. 10 D. 11

试题 10

某项目组拟开发一个大规模系统，且具备了相关领域及类似规模系统的开发经验。下列过程模型中，（10）最合适开发此项目。

- (10) A. 原型模型 B. 瀑布模型 C. V 模型 D. 螺旋模型

3.3.3 解析与答案

试题 1 分析

代码行技术（LOC）是比较简单的定量估算软件规模的方法。它的计算过程是：首先由多名有经验的软件工程师分别估计出软件的最小规模（ a ）、最大规模（ b ）和最可能的规模（ p ），然后分别计算三种规模的平均值 α 、 β 和 θ ，最后代入公式 $L=(\alpha+4\theta+\beta)/6$ ，就可以得出程序规模的估计值 L 。

试题 1 答案

- (1) A

试题 2 分析

甘特图的优点是直观表明各个任务的计划进度和当前进度，能动态地反映软件开发进展的情况，是小型项目中常用的工具。缺点是不能显式地描绘各个任务间的依赖关系，关键任务也不明确。

试题 2 答案

- (2) C

试题 3 分析

CMM 为软件企业的过程能力提供了一个阶梯式的进化框架，将软件过程改进的进化步骤组织成 5 个成熟度等级，每一个级别定义了一组过程能力目标，并描述了要达到这些目标应该采取的实践活动，为不断改进过程奠定了循序渐进的基础。

初始级，企业一般缺少有效的管理，不具备稳定的软件开发与维护的环境。软件过程是未加定义的随意过程，项目的执行随意甚至是混乱的，几乎没有定义过程的规则（或步骤）。

可重复级，企业建立了基本的项目管理过程的政策和管理规程，对成本、进度和功能进行监控，以加强过程能力。

定义级，企业全面采用综合性的管理及工程过程来管理，对整个软件生命周期的管理与工程化过程都已标准化，并综合成软件开发企业标准的软件过程。

管理级，企业开始定量地认识软件过程，软件质量管理和软件过程管理是量化的管理。对软件过程与产品质量建立了定量的质量目标，制定了软件过程和产品质量的详细而具体的度量标准，实现了度量标准化。

优化级，企业将会把工作重点放在对软件过程改进的持续性、预见及增强自身，防止缺陷及问题的发生，不断地提高过程处理能力上。通过来自过程执行的质量反馈和吸收新方法和新技术的定量分析来改善下一步的执行过程，即优化执行步骤，使软件过程能不断地得到改进。

试题 3 答案

(3) A

试题 4 分析

本题主要考查项目管理中进度管理的网络图方面的知识。题目给出的工程网络图表示各个任务完成需要的时间以及相互依存的关系，整个工程的工期就是网络图中关键路径上各个任务完成时间的总和。就本题而言，关键路径是①—②—③—⑤—⑥，历时 23 天。

试题 4 答案

(4) A

试题 5 分析

本题考查 ISO/IEC 9126 软件质量模型中第一层定义的可靠性。可靠性包括成熟性、容错性和易恢复性子特性。子特性易理解性和易学性属于易使用性，子特性准确性属性功能性。

试题 5 答案

(5) C

试题 6 分析

本题考查项目计划的关键路径。不难看出，图中任务流 A→B→C→D→I 所需天数为 19，任务流 A→B→C→E→I 所需天数为 18，任务流 A→B→C→F→G→I 所需天数为 17，任务流 A→B→C→F→H→I 所需天数为 16，因此任务流 A→B→C→D→I 为关键路径，完成项目所需的最短时间是 19 天。

试题 6 答案

(6) A

试题 7 分析

本题考查软件能力成熟度模型（CMM）的成熟度等级。CMM 将软件过程能力成熟度划分为 5 级，每一级都为下一级提供一个基础。管理级对软件过程和产品都有定量的理解与控制，因此管理级和优化级均对软件过程和产品有定量的理解与控制。

试题 7 答案

(7) C

试题 8 分析

本题考查项目管理基础知识。在规划软件开发资源时为了确定系统开发所需的人员数量,需要综合考虑软件系统的规模、系统的技术复杂性、项目计划和开发人员的技术背景等方面。系统的市场前景与开发管理人员无关,主要是决策者和销售者所关心的事情。

试题 8 答案

(8) A

试题 9 分析

计算如下。先计算每个任务的最早时间:2号开始的最早时间是 $0+2=2$,5号是 $2+2=4$,7号是 $4+5=9$,3号是 $0+2=2$,4号是0、6的两个前驱任务3、4中取最迟的,则是4,8号的两个前驱任务是5和6,取最迟的是9,9的两个前驱是7、8,取最迟的时间是15。

接下来计算最迟开始时间,9号任务的最迟时间是15,就是最早开工时间,因为9是最后一个任务了。倒过来计算7的最迟时间是 $15-6=9$,8号的最迟时间是 $15-4=11$,8号的前驱是6,因此6的最迟时间是 $11-1=10$ 。其余以此类推即可。

试题 9 答案

(9) C

试题 10 分析

本题考查对软件开发生命周期模型的基本知识。

常见的软件生存周期模型有瀑布模型、演化模型、螺旋模型、喷泉模型等。瀑布模型是将软件生存周期各个活动规定为依线性顺序连接的若干阶段的模型,适合于软件需求很明确的软件项目的模型。V模型是瀑布模型的一种演变模型,将测试和分析与设计关联进行,加强分析与设计的验证。原型模型是一种演化模型,通过快速构建可运行的原型系统,然后根据运行过程中获取的用户反馈进行改进。演化模型特别适用于对软件需求缺乏准确认识的情况。螺旋模型将瀑布模型和演化模型结合起来,加入了两种模型均忽略的风险分析。

本题中项目组具备了所开发系统的相关领域及类似规模系统的开发经验,即需求明确,瀑布模型最适合开发此项目。

试题 10 答案

(10) B

3.4 考前冲刺

试题 1

软件产品的可靠性并不取决____(1)____。

- (1) A. 潜在错误的数量 B. 潜在错误的位置
C. 软件产品的使用方式 D. 软件产品的开发方式

试题 2

模块 A 直接访问模块 B 的内部数据,则模块 A 和模块 B 的耦合类型为____(2)____。

- (2) A. 数据耦合 B. 标记耦合 C. 公共耦合 D. 内容耦合

试题 3

下列关于风险的叙述不正确的是:风险是____(3)____。

- (3) A. 可能发生的事件
B. 一定会发生的事件
C. 会带来损失的事件
D. 可能对其进行干预, 以减少损失的事件

试题 4

下列关于项目估算方法的叙述不正确的是 (4) 。

- (4) A. 专家判断方法受到经验和主观性影响
B. 启发式方法 (如 COCOMO 模型) 的参数难以确定
C. 机器学习方法难以描述训练数据的特征和确定其相似性
D. 结合上述三种方法可以得到精确的估算结果

试题 5

一个软件项目的活动图如图 3-12 所示, 其中顶点表示项目里程碑, 边表示包含的活动, 边上的权重表示活动的持续时间, 则里程碑 (5) 在关键路径上。

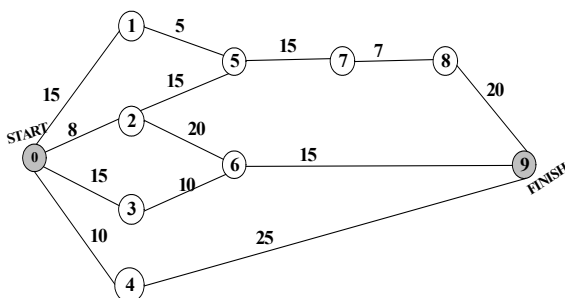


图 3-12 某软件项目活动图

- (5) A. 1 B. 2 C. 3 D. 4

试题 6

软件风险一般包含 (6) 两个特征。

- (6) A. 救火和危机管理 B. 已知风险和未知风险
C. 不确定性和损失 D. 员工和预算

试题 7

面向对象开发方法的基本思想是尽可能按照人类认识客观世界的方法来分析和解决问题, (7) 方法不属于面向对象方法。

- (7) A. Booch B. Coad C. OMT D. Jackson

试题 8

程序的 3 种基本控制结构是 (8) 。

- (8) A. 过程、子程序和分程序 B. 顺序、选择、重复
C. 递归、堆栈、队列 D. 调用、返回、跳转

试题 9

栈是一种按后进先出原则插入和删除操作的数据结构, 因此 (9) 必须用栈。

- (9) A. 函数或过程进行递归调用及返回处理 B. 将一个元素序列进行逆置
C. 链表节点的申请和释放 D. 可执行程序的装入和卸载

试题 10

软件开发中的瀑布模型典型地刻画了软件生命周期的阶段划分，与其最适应的软件开发方法是（10）。

- (10) A. 构件化方法 B. 结构化方法 C. 面向对象方法 D. 快速原型法

试题 11

利用结构化分析模型进行接口设计时，应以（11）为依据。

- (11) A. 数据流图 B. 实体关系图 C. 数据字典 D. 状态迁移图

试题 12

确定软件的模块划分及模块之间的调用关系是（12）阶段的任务。

- (12) A. 需求分析 B. 概要设计 C. 详细设计 D. 编码

试题 13

以下关于类继承的说法中，错误的是（13）。

- (13) A. 通过类继承，在程序中可以复用基类的代码
B. 在继承类中可以增加新代码
C. 在继承类中不能定义与被继承类（基类）中的方法同名的方法
D. 在继承类中可以覆盖被继承类（基类）中的方法

试题 14

软件开发的增量模型（14）。

- (14) A. 最适用于需求被清晰定义的情况
B. 是一种能够快速构造可运行产品的好方法
C. 最适合于大规模团队开发的项目
D. 是一种不适用于商业产品的创新模型

试题 15

采用 UML 进行软件设计时，可用（15）关系表示两类实体之间存在的特殊/一般关系，用聚集关系表示事物之间存在的整体/部分关系。

- (15) A. 依赖 B. 聚集 C. 泛化 D. 实现

3.5 习题解析

试题 1 分析

软件产品的可靠性取决于潜在错误的数量、潜在错误的位置以及软件产品的使用方式，但不包括软件产品的开发方式。

软件可靠性与软件缺陷有关，也与系统输入和系统使用有关。理论上说，可靠的软件系统应该是正确、完整、一致和健壮的。但是实际上任何软件都不可能达到百分之百的正确，而且也无法精确度量。一般情况下，只能通过对软件系统进行测试来度量其可靠性。

这样，给出如下定义：“软件可靠性是软件系统在规定的时间内及规定的环境条件下，完成规定功能的能力”。根据这个定义，软件可靠性包含了以下三个要素。

① 规定的时间

软件可靠性只是体现在其运行阶段，所以将“运行时间”作为“规定的时间”的度量。“运行时间”包括软件系统运行后工作与挂起（开启但空闲）的累计时间。由于软件运行的环境与程序路径选取的随机性，软件的失效为随机事件，所以运行时间属于随机变量。

② 规定的环境条件

环境条件指软件的运行环境。它涉及软件系统运行时所需的各种支持要素，如支持硬件、

操作系统、其他支持软件、输入数据格式和范围以及操作规程等。不同的环境条件下软件的可靠性是不同的。具体地说，规定的环境条件主要是描述软件系统运行时计算机的配置情况以及对输入数据的要求，并假定其他一切因素都是理想的。有了明确规定的环境条件，还可以有效判断软件失效的责任在用户方还是研制方。

③ 规定的功能

软件可靠性还与规定的任务和功能有关。由于要完成的任务不同，软件的运行剖面会有所区别，则调用的子模块就不同（即程序路径选择不同），其可靠性也就可能不同。所以要准确度量软件系统的可靠性必须首先明确它的任务和功能。

试题 1 答案

(1) D

试题 2 分析

软件工程中对象之间的耦合度就是对象之间的依赖性。指导使用和维护对象的主要问题是对象之间的多重依赖性。对象之间的耦合越高，维护成本越高。因此对象的设计应使类和构件之间的耦合最小，耦合性由低到高分别是：非直接耦合、数据耦合、标记耦合、控制耦合、外部耦合、公共耦合、内容耦合。当一个模块直接修改或操作另一个模块的数据，或者直接访问入另一个模块时，就发生了内容耦合。

试题 2 答案

(2) D

试题 3 分析

风险涉及一个事件发生的可能性，涉及该事件产生的不良后果或影响。

试题 3 答案

(3) B

试题 4 分析

项目估算的常用方法主要有专家判断法、启发式法和机器学习法等。

专家判断法是指向学有专长、见识广博并有相关经验的专家进行咨询、根据他们多年来的实践经验和判断能力对计划项目做出预测的方法。很显然，采用这种方法容易受到专家经验和主观性的影响。

启发式方法使用一套相对简单、通用、有启发性的规则进行估算的方法，它具有参数难以确定、精确度不高等特点。

机器学习方法是一种基于人工智能与神经网络技术的估算方法，它难以描述训练数据的特征和确定其相似性。

而无论采用哪种估算方法，估算得到的结果都是大概的，而不是精确的。

试题 4 答案

(4) D

试题 5 分析

本题主要考查关键路径求解的问题。

从开始顶点到结束顶点的最长路径为关键路径（临界路径），关键路径上的活动为关键活动。

在本题中找出的最长路径是 Start→2→5→7→8→Finish，其长度为 $8+15+15+7+20=65$ ，而其他任何路径的长度都比这条路径小，因此我们可以知道里程碑 2 在关键路径上。

试题 5 答案

(5) B

试题 6 分析

这是一道软件风险概念题，软件风险包括不确定性和损失两个特征。不确定性指风险有可能发生，也可能不发生；损失是当风险确实发生时所引起的不希望的损失或结果。救火和危机管理是对不合适，但经常采用的软件风险管理策略，已知风险和未知风险是对软件风险进行分类的一种方式，员工和预算是在识别项目风险时需要识别的因素。

试题 6 答案

(6) C

试题 7 分析

本题考查面向对象开发方法，该方法有 Booch、Coad 和 OMT 方法，Jackson 是一种面向数据结构的开发方法。

试题 7 答案

(7) D

试题 8 分析

本题考查的是结构化程序设计中的 3 种基本控制结构，是一道概念题。选择也称为“判断”，重复也称为“循环”。

试题 8 答案

(8) B

试题 9 分析

栈结构最大的特点就是后进先出，因此非常适合函数的递归调用和及时返回。

试题 9 答案

(9) A

试题 10 分析

结构化的分析与设计的软件开发方法是采用结构化技术来完成软件开发的各项任务。该方法把软件生命周期的全过程依次划分为若干阶段，然后顺序地完成每个阶段的任务，与瀑布模型有很好的结合度，是与其最相适应的开发方法。

试题 10 答案

(10) B

试题 11 分析

数据流图是结构化分析模型需求分析阶段得到的结果，描述了系统的功能，在进行接口设计时，应以它为依据。

试题 11 答案

(11) A

试题 12 分析

需求分析阶段的任务主要是要解决系统做什么的问题，即弄清楚问题的要求，包括需要输入什么数据，要得到什么结果，最后应输出什么。

概要设计的主要任务是把需求分析得到的结果转换为软件结构和数据结构，即将一个复杂系统按功能进行模块划分，建立模块的层次结构及调用关系，确定模块间的接口及人机界

面，确定数据的结构特性及数据库的设计等。

详细设计是在概要设计的基础上进行更细致的设计，它包括具体的业务对象设计、功能逻辑设计、界面设计等工作。详细设计是系统实现的依据，需要更多地考虑设计细节。

编码即编写程序代码，具体实现系统。

试题 12 答案

(12) B

试题 13 分析

在继承类中可以定义与被继承类（基类）中的方法同名的方法。

试题 13 答案

(13) C

试题 14 分析

增量模型与原型实现模型和其他演化方法一样，本质上是迭代的，但与原型实现不一样的是其强调每一个增量均发布一个可操作产品。采用增量模型的优点是人员分配灵活，刚开始不用投入大量人力资源。如果核心产品很受欢迎，则可增加人力实现下一个增量。当配备的人员不能在设定的期限内完成产品时，它提供了一种先推出核心产品的途径。这样即可先发布部分功能给客户，对客户起到镇静剂的作用。此外，增量能够有计划地管理技术风险。是一种能够快速构造可运行产品的好方法。

试题 14 答案

(14) B

试题 15 分析

本题考查 UML 实体间联系的概念。UML 实体间相互关系有如下 4 种。

① 依赖关系：假设 A 类的变化引起了 B 类的变化，则说明 B 类依赖于 A 类。依赖关系有如下 3 种情况。

A 类是 B 类的一个成员变量；

A 类是 B 类方法中的一个参数；

A 类向 B 类发送消息，从而影响 B 类发生情况。

② 泛化关系：A 是 B 和 C 的父类，B 和 C 具有公共类（父类）A，说明 A 是 B 和 C 的一般化也称泛化。在 UML 中对泛化关系有如下 3 个要求。

子类与父类应该完全一致，父类所具有的属性和操作，子类应该都有；

子类中除了与父类一致的信息以外，还包括额外的信息；

可以使用父类的实例处也可以使用子类的实例。

③ 聚集关系：聚集关系是所有关系当中最通用的关系，指的是两个类的实例之间存在某种语义上的联系且这种联系不存在非常明确的定义，如学校、教室、老师。聚集关系分为如下两种。

聚合关系，即整体与部分的关系，二者可以分开；

组合关系，即整体与部分的关系，二者不可以分开。

④ 实现关系：用来规定接口和实现接口的类或者构建结构的关系，接口是操作的集合，而这些操作用于规定类或者构建的一种服务。

试题 15 答案

(15) C

知识经济时代，知识产权作为一个企业乃至国家提高核心竞争力的战略资源，凸现出前所未有的重要地位。标准化工作是信息化建设中的一项基础性的系统工程，是信息系统开发成功和得以推广应用的关键之一，因此，加强信息标准化工作具有十分重要的现实意义和深远的历史意义。

4.1 考点脉络

知识产权与标准化是网络工程师考试中一个必考的内容。根据考试大纲，要求考生掌握以下两个方面的内容。

- (1) 知识产权：包括知识产权保护、著作权、专利权保护等。
- (2) 标准化：标准化法。

从历年的考试试题来看，本章的考点在综合知识考试中的平均分数为 1 分，约为总分的 1.3%。考试试题分数主要集中在知识产权保护、著作权、专利权保护这 3 个知识点上。

4.2 知识产权

在知识产权这个考点中，主要涉及《中华人民共和国著作权法》、《中华人民共和国著作权法专利法》、《计算机软件保护条例》、《中华人民共和国反不正当竞争法》这 4 部法律条文的内容。

4.2.1 考点精讲

国家制定著作权法是为了保护作者的权益，同时还在于鼓励作品得到广泛的传播，繁荣社会的文化生活。专利法的目的在于保护发明创造专利权，鼓励发明创造，促进科学技术进步和创新。计算机软件保护条例是为了保护计算机软件著作权人的权益，调整计算机软件在开发、传播和使用中发生的利益关系，鼓励计算机软件的开发与流通，促进计算机应用事业的发展。反不正当竞争法是一部旨在规范社会主义市场经济秩序，倡导公平有序竞争的法律。

1. 著作权法

《中华人民共和国著作权法》是知识产权保护领域的最重要的法律基础，现行的是 2002 年 9 月修订的版本。

(1) 著作权法客体

著作权法及实施条件的客体是指受保护的作品。这里的作品，是指文学、艺术和自然科学、社会科学、工程技术领域内具有独创性并能以某种有形形式复制的智力成果。

① 作品类型

作品包括以下 9 种类型。

- a. 文字作品：包括小说、诗词、散文、论文等以文字形式表现的作品。
- b. 口述作品：是指即兴的演说、授课、法庭辩论等以口头语言形式表现的作品。
- c. 音乐、戏剧、曲艺、舞蹈、杂技作品。
- d. 美术、摄影作品。
- e. 电影、电视、录像作品。
- f. 工程设计、产品设计图纸及其说明。
- g. 地图、示意图等图形作品。
- h. 计算机软件。
- i. 法律、行政法规规定的其他作品。

② 职务作品

为完成单位工作任务所创作的作品，称为职务作品。如果该职务作品是利用单位的物质技术条件进行创作，并由单位承担责任的，或者有合同约定，其著作权属于单位。那么作者将仅享有署名权，其他著作权归单位享有。

其他职务作品，著作权仍由作者享有，单位有权在业务范围内优先使用。并且在两年内，未经单位同意，作者不能够许可其他人、其他单位使用该作品。

(2) 著作权法主体

著作权法及实施条例的主体是指著作权关系人，通常包括著作权人、受让者。

① 著作权人与受让者

a. 著作权人，又称为原始著作权人，是根据创作的事实进行确定的，创作、开发者将依法取得著作权人资格。

b. 受让者，又称为后继著作权人，是指没有参与创作，通过著作权转移活动成为享有著作权的人。

② 著作权人的确定

著作权法在认定著作权人时，是根据创作的事实进行的，而创作就是指直接产生文学、艺术和科学作品的智力活动。而为他人创作进行组织，提供咨询意见、物质条件或者进行其他辅助工作的，不属于创作的范围，不被确认为著作权人。

如果在创作的过程中，有多人参与，那么该作品的著作权将由合作的作者共同享有。合作的作品是可以分割使用的，作者对各自创作的部分可以单独享有著作权，但不能够在侵犯合作作品整体的著作权的情况下行使。

而如果遇到作者不明的情况，那么作品原件的所有人可以行使除署名权以外的著作权，直到作者身份明确。

另外值得注意的是，如果作品是委托创作的话，著作权的归属应通过委托人和受托人之间的合同来确定。如果没有明确的约定，或者没有签订相关合同，则著作权仍属于受托人。

(3) 著作权

根据著作权法及实施条例规定，著作权人对作品享有 5 种权利。

- a. 发表权：即决定作品是否公之于众的权利。

- b. 署名权：即表明作者身份，在作品上署名的权利。
- c. 修改权：即修改或者授权他人修改作品的权利。
- d. 保护作品完整权：即保护作品不受歪曲、篡改的权利。
- e. 使用权、使用许可权和获取报酬权、转让权：即以复制、表演、播放、展览、发行、摄制电影、电视、录像或者改编、翻译、注释、编辑等方式使用作品的权利，以及许可他人以上述方式使用作品，并由此获得报酬的权利。

① 著作权保护期限

根据著作权法相关规定，著作权的保护是有一定期限的。

a. 著作权属于公民。署名权、修改权、保护作品完整权的保护期没有任何限制，永远属于保护范围。而发表权、使用权和获得报酬权的保护期为作者终生及其死亡后的 50 年（第 50 年的 12 月 31 日）。作者死亡后，著作权依照继承法进行转移。

b. 著作权属于单位。发表权、使用权和获得报酬权的保护期为 50 年（首次发表后的第 50 年的 12 月 31 日），若 50 年内未发表的，不予保护。但单位变更、终止后，其著作权由承受其权利义务的单位享有。

② 使用许可

当第三方需要使用作品时，需得到著作权人的使用许可，双方应签订相应的合同。合同中应包括许可使用作品的方式、是否专有使用、许可的范围与时间期限、报酬标准与方法、违约责任。在合同未明确许可的权力时，需再次经著作权人许可。合同的有效期限不超过 10 年，期满时可以续签。

对于出版者、表演者、录音录像制作者、广播电台、电视台而言，在下列情况下使用作品，可以不经著作权人许可，不向其支付报酬。但应指出作者姓名、作品名称。

- a. 为了个人学习、研究或者欣赏，使用他人已经发表的作品。
- b. 为了介绍、评论某一个作品或者说明某一个问题，在作品中适当引用他人已经发表的作品。
- c. 为了报道时间新闻，在报纸、期刊、广播、电视节目或者新闻纪录影片中引用已经发表的作品。
- d. 报纸、期刊、广播电台、电视台刊登或者播放其他报纸、期刊、广播电台、电视台已经发表的社论、评论员文章。
- e. 报纸、期刊、广播电台、电视台刊登或者播放在公众集会上发表的讲话，但作者声明不许刊登、播放的除外。
- f. 为了学校课堂教学或者科学研究，翻译或者少量复制已经发表的作品，供教学或者科研人员使用，但不得出版发行。
- g. 国家机关为执行公务使用已经发表的作品。
- h. 图书馆、档案馆、纪念馆、博物馆、美术馆等为了陈列或者保存版本的需要，复制本馆收藏的作品。
- i. 免费表演已经发表的作品。
- j. 对设置或者陈列在室外公共场所的艺术作品进行临摹、绘画、摄影、录像。
- k. 将已经发表的汉族文字作品翻译成少数民族文字在国内出版发行。

1. 将已经发表的作品改成盲文出版。

2. 专利法

《中华人民共和国专利法》是我国对专利技术保护的法律基础，现行的是 2009 年 10 月 1 日正式实施的新版本。

(1) 专利法的保护对象

专利法的客体是发明创造，也就是其保护的对象。这里的发明创造是指发明、实用新型和外观设计。

① 发明：就是指对产品、方法或者其改进所提出的新的技术方案。

② 实用新型：是指对产品的形状、构造及其组合，提出的实用的新的技术方案。

③ 外观设计：对产品的形状、图案及其组合，以及色彩与形状、图案的结合所做出的富有美感并适于工业应用的新设计。

(2) 确定专利权人

根据专利法的规定，专利权归属于发明人或者设计人，就是指对发明创造做出创造性贡献的人。对于在发明创造过程中，只负责组织、提供方便、从事辅助工作的都不属于发明人或设计人。

① 职务发明

如果是执行单位任务，或者是利用本单位的物质技术条件所完成的发明创造，被视为职务发明创造，通常包括：

a. 在本职工作中做出的发明创造。

b. 在履行单位交付的本职工作之外的任务中所做出的发明创造。

c. 辞职、退休或者调动工作后 1 年内做的，与其原来承担的任务相关的发明创造。

对于职务发明的专利申请被批准后，单位是专利权人。对于利用单位的物质技术条件进行发明创造的，发明人、设计人与单位之间可以签订合同，重新规定专利权的归属。

② 合作发明、设计

对于合作发明、设计的，其专利权应属共同所有，但可以根据合作方之间另行签订的合同来确定专利权的归属。

③ 委托发明

一个单位或者个人接受其他单位或个人的委托，所完成的发明创造，若没有签订合同规定专利权归属，则专利权归属发明、设计者。

④ 其他

如果非职务发明，则单位无权压制个人进行专利权申请。对于多个相类似的专利申请，专利权归属最先提交的申请人。

(3) 专利权

① 专利权保护

未经专利权人许可，实施专利的，就属于侵犯专利权，专利权人可以起诉，申请调解。

a. 假冒他人专利，没收违法所得，并处于 3 倍以下的罚款，或 5 万元以下罚款，情节严重的，依法追究刑事责任。

b. 以非专利产品冒充专利产品，责令整改，并处以 5 万元以下的罚款。

- c. 侵犯专利权的赔偿数额，参照该专利许可使用费的倍数合理确定。
- d. 专利诉讼的有效期限是 2 年，以专利权人得知侵权行为之日起计算。
- e. 对于以下情况，不视为侵犯专利权：

对于专利权人制造、进口或者经专利权人许可而制造、进口的专利产品，或者依照专利方法直接获得的产品售出后，使用、许诺销售或者销售该产品。

在专利申请日前已经制造相同产品、使用相同方法或者已经做好制造、使用的必要准备，并且供在原有范围内继续制造、使用。

临时通过中国的国外运输工具，在其自身需要时使用的专利。

专为科学研究和实验而使用有关专利。

② 专利权保护期限

我国现行《专利法》规定的发明专利权保护期限为 20 年，实用新型和外观设计专利权的期限为 10 年，均从申请日开始计算。在保护期内，专利权人应该按时缴纳年费。

在专利权保护期限内，如果专利权人没有按规定缴纳年费，或以书面声明放弃其专利权的，专利权可以在期满前终止。

另外，任何单位和个人都可以在授予专利之日起，请求专利复审，如果复审未通过，则将终止专利权。

3. 计算机软件保护条例

《计算机软件保护条例》是我国计算机软件保护的法律法规，该条例最新版本是在 2001 年年底通过，从 2002 年 1 月 1 日起正式实施的。

由于计算机软件也属于《中华人民共和国著作权法》保护的范畴，因此在具体实施时，首先适用于《计算机软件保护条例》条文规定，若是在《计算机软件保护条例》中没有规定适用条文的情况下，才依据《著作权法》的原则和条文规定执行。

(1) 保护对象

《计算机软件保护条例》的客体是计算机软件，而在此计算机软件是指计算机程序及其相关文档。

根据条例规定，受保护的软件必须是由开发者独立开发的，并且已经固定在某种有形物体上（如光盘、硬盘、软盘）。

另外要注意的是，其对软件著作权的保护只是针对计算机软件和文档，并不包括开发软件所用的思想、处理过程、操作方法或数学概念等。并且著作权人还需在软件登记机构办理登记。

(2) 著作权人确定

对于由两个以上开发者或组织合作开发的软件，著作权的归属根据合同约定确定。若无合同，共享著作权。若合作开发的软件可以分割使用，那么开发者对自己开发的部分单独享有著作权，可以在不破坏整体著作权的基础上行使。

如果开发者在单位或组织中任职期间，所开发的软件若符合以下条件的，则软件著作权应归单位或组织所有。

- ① 针对本职工作中明确规定的开发目标所开发的软件。
- ② 开发出的软件属于从事本职工作活动的结果。

③ 使用了单位或组织的资金、专用设备、未公开的信息等物质、技术条件，并由单位或组织承担责任的软件。

如果是接受他人委托而进行开发的软件，其著作权的归属应由委托人与受托人签订书面合同约定；如果没有签订合同，或合同中未规定的，其著作权由受托人享有。

另外，由国家机关下达任务开发的软件，著作权的归属由项目任务书或合同规定；若未明确规定，其著作权应归任务接受方所有。

（3）软件著作权

根据《计算机软件保护条例》规定，软件著作权人对其创作的软件产品，享有以下 9 种权利。

- a. 发表权：即决定软件是否公之于众的权利。
- b. 署名权：即表明开发者身份，在软件上署名的权利。
- c. 修改权：即对软件进行增补、删节，或者改变指令、语句顺序的权利。
- d. 复制权：即将软件制作一份或者多份的权利。
- e. 发行权：即以出售或者赠予方式向公众提供软件的原件或者复制件的权利。
- f. 出租权：即有偿许可他人临时使用软件的权利。
- g. 信息网络传播权：即以信息网络方式向公众提供软件的权利。
- h. 翻译权：即将原软件从一种自然语言文字转换成另一种自然语言文字的权利。
- i. 使用许可权、获得报酬权、转让权。

软件著作权自软件开发完成之日起生效。

① 著作权属于公民。著作权的保护期为作者终生及其死亡后的 50 年（第 50 年的 12 月 31 日）。对于合作开发的，则以最后死亡的作者为准。值得注意的是，在 1991 年实施的上一版条例中，保护期限是 25 年；而在最新的条例中，则已经改为了 50 年。在作者死亡后，将根据继承法转移除了署名权之外的著作权。

② 著作权属于单位。著作权的保护期为 50 年（首次发表后的第 50 年的 12 月 31 日），若 50 年内未发表的，不予保护。但单位变更、终止后，其著作权由承受其权利义务的单位享有。

当得到软件著作权人的许可，获得了合法的计算机软件复制品时，则复制品的所有人享有以下权利。

① 根据使用的需求，将该计算机软件安装到设备中（计算机、PDA 等信息设备）。

② 可以制作复制品的备份，以防止复制品损坏，但这些复制品不得通过任何方式转给其他人使用。

③ 根据实际的应用环境，对其进行功能、性能等方面的修改。但未经软件著作权人许可，不得向任何第三方提供修改后的软件。

如果使用者只是为了学习、研究软件中包含的设计思想、原理，而以安装、显示、存储软件等方式使用软件，可以不经软件著作权人许可，不向其支付报酬。

（4）法律责任

有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任。

- ① 未经软件著作权人许可，发表或者登记其软件的。
- ② 将他人软件作为自己的软件发表或者登记的。
- ③ 未经合作者许可，与他人合作开发的软件作为自己单独完成的软件发表或者登记的。
- ④ 在他人软件上署名或者更改他人软件上的署名的。
- ⑤ 未经软件著作权人许可，修改、翻译其软件的。
- ⑥ 其他侵犯软件著作权的行为。

未经软件著作权人许可，有下列侵权行为的，应当根据情况，承担停止侵害、消除影响、赔礼道歉、赔偿损失等民事责任；同时损害社会公共利益的，由著作权行政管理部门责令停止侵权行为，没收违法所得，没收、销毁侵权复制品，并处罚款；情节严重的，著作权行政管理部门可以没收主要用于制作侵权复制品的材料、工具、设备等；触犯刑律的，依照刑法关于侵犯著作权罪、销售侵权复制品罪的规定，依法追究刑事责任。

- ① 复制或者部分复制著作权人的软件的。
- ② 向公众发行、出租，通过信息网络传播著作权人的软件的。
- ③ 故意避开或者破坏著作权人为保护其软件著作权而采取的技术措施的。
- ④ 故意删除或者改变软件权利管理电子信息的。
- ⑤ 转让或者许可他人行使著作权人的软件著作权的。

软件著作权人有证据证明他人正在实施或者即将实施侵犯其权利的行为，如不及时制止，将会使其合法权益受到难以弥补的损害的，可以依照《中华人民共和国著作权法》的规定，在提起诉讼前向人民法院申请采取责令停止有关行为和财产保全的措施。

为了制止侵权行为，在证据可能灭失或者以后难以取得的情况下，软件著作权人可以依照《中华人民共和国著作权法》的规定，在提起诉讼前向人民法院申请保全证据。

软件复制品的出版者、制作者不能证明其出版、制作有合法授权的，或者软件复制品的发行者、出租者不能证明其发行、出租的复制品有合法来源的，应当承担法律责任。

软件开发者开发的软件，由于可供选用的表达方式有限而与已经存在的软件相似的，不构成对已经存在的软件的著作权的侵犯。

软件的复制品持有人不知道也没有合理理由应当知道该软件是侵权复制品的，不承担赔偿责任；但是，应当停止使用、销毁该侵权复制品。如果停止使用并销毁该侵权复制品将给复制品使用人造成重大损失的，复制品使用人可以在向软件著作权人支付合理费用后继续使用。

4. 反不正当竞争法

《中华人民共和国反不正当竞争法》的实施目的是为了维护市场的公平环境，制止不正当竞争行为，现行的是 1993 年 12 月 1 日正式实施的版本。

(1) 什么是不正当竞争

不正当竞争是指经营者违反本法规定，损害其他经营者的合法权益，扰乱社会经济秩序的行为。

① 采用不正当的市场交易手段：采用例如假冒他人注册商标；擅自使用与知名商品相同或相近的名称、包装，混淆消费者；擅自使用他人的企业名称；在商品上伪造认证标志、名优标志、产地等信息，从而达到损害其他经营者的目的。

② 利用垄断的地位，来排挤其他经营者的公平竞争。

③ 利用政府职权，限定商品购买，以及对商品实施地方保护主义。

④ 利用财务或其他手段进行贿赂，以达到销售商品的目的。

⑤ 利用广告或者其他方法，对商品的质量、成分、性能、用途、生产者、有效期、产地等进行误导性的虚假宣传。

⑥ 以低于成本价进行销售，以排挤竞争对手。不过对于鲜活商品、有效期将至及积压产品的处理，以及季节性降价，因清债、转产、歇业等原因进行降价销售的均不属于不正当竞争。

⑦ 搭售违背购买者意愿的商品。

⑧ 采用不正当的有奖销售。例如谎称有奖，却是内定人员中奖；利用有奖销售推销质次价高产品；奖金超过 5000 元的抽奖式有奖销售。

⑨ 捏造、散布虚伪事实，损害对手商誉。

⑩ 串通投标，排挤对手。

(2) 法律责任

采用不正当竞争对别的经营者造成损害的，应承担赔偿责任。如果无法计算损失的，则赔偿侵权期因侵权所得的利润。

① 对于假冒注册商标、姓名、认证、产地的不正当竞争行为根据《商标法》进行处罚；如果是仿冒知名商标的，则可以根据情节罚款违法所得的 1~3 万元罚款，特别严重的追究刑事责任。

② 通过贿赂达到销售目的，根据情节处以 1~20 万元罚款，严重的追究刑事责任。

③ 利用独占地位进行经营，根据情节处以 5~20 万元罚款；借此销售质次价高商品的，则没收违法所得，并罚款 1~3 万元。

④ 采用广告误导消费者，处于 1~20 万元罚款。

⑤ 采用不合法的有奖销售的，根据情节处以 1~10 万元的罚款。

⑥ 串通投标者，根据情节处以 1~20 万元的罚款。

(3) 商业秘密

商业秘密是指不为公众所知，具有经济利益，具有实用性，并且已经采取了保密措施的技术信息与经营信息。在《反不正当竞争法》中对商业秘密进行了保护，如果存在以下行为的，视为侵犯商业秘密。

① 以盗窃、利诱、胁迫等不正当手段获取别人的商业秘密。

② 披露、使用不正当手段获取的商业秘密。

③ 违反有关保守商业秘密的要求约定，披露、使用其掌握的商业秘密。

对于侵犯商业秘密的，将根据情节处于 1~20 万元罚款。

4.2.2 一点一练

试题 1

两个以上的是申请人分别就相同内容的计算机程序的发明创造，先后向国务院专利行政部门提出申请， (1) 可以获得专利申请权。

(1) A. 所有的申请人 B. 先申请人 C. 先使用人 D. 先发明人

试题 2

我国著作权法中，____(2)____系指同一概念。

- (2) A. 出版权与版权 B. 著作权与版权 C. 作者权与专有权 D. 发行权与版权

试题 3

某软件设计师自行将他人使用 C 程序语言开发的控制程序转换为机器语言形式的控制程序，并固化在芯片中，该软件设计师的行为____(3)____。

- (3) A. 不构成侵权，因为新的控制程序与原控制程序使用的程序设计语言不同
B. 不构成侵权，因为对原控制程序进行了转换与固化，其使用和表现形式不同
C. 不构成侵权，将一种程序语言编写的源程序转换为另一种程序语言形式，是“翻译”行为
D. 构成侵权，因为他不享有原软件作品的著作权

试题 4

____(4)____不需要登记或标注版权标记就能得到保护。

- (4) A. 专利权 B. 商标权 C. 著作权 D. 财产权

试题 5

依据著作权法，计算机软件著作权保护的对象是指____(5)____。

- (5) A. 计算机硬件 B. 计算机软件
C. 计算机硬件和软件 D. 计算机文档

4.2.3 解析与答案

试题 1 分析

对于专利权而言，若有多个相类似的专利申请，专利权归属最先提交的申请人，这在《专利法》中有专门的说明。

试题 1 答案

- (1) B

试题 2 分析

本题考核有关著作权概念的知识。著作权又称为版权，前者属于大陆法系著作权法的称谓，后者则起源于英美法系。我国在进行著作权立法时就采取大陆法系著作权模式，同时也不排斥英美版权法模式。因此我国 2001 年新修订的著作权法和 1990 年原著作权法第 51 条分别规定“本法所称著作权与版权系同义语”和“本法所称著作权即版权”。可见，我国著作法中著作权和版权系同一概念。

试题 2 答案

- (2) B

试题 3 分析

根据《中华人民共和国计算机软件保护条例》的规定，软件著作权人享有翻译权，即将原软件从一种自然语言文字转换成另一种自然语言文字的权利。未经软件著作权人许可，发表或者登记其软件的行为，构成计算机软件侵权。

试题 3 答案

- (3) D

试题 4 分析

无形的智力创造性成果不像有形财产那样直观可见，因此，确认智力创造性成果的财产权需要依法审查确认得到法律保护。例如，我国的发明人所完成的发明，其实用新型或者外观设计，已经具有价值和使用价值，但是其完成人尚不能自动获得专利权。完成人必须依照专利法的有关规定，向国家专利局提出专利申请。专利局依照法定程序进行审查，申请符合专利法规定条件的，由专利局做出授予专利权的决定，颁发专利证书。只有当专利局发布授权公告后，其完成人才享有该项知识产权。又如，商标权的获得，我国和大多数国家实行注册制，只有向国家商标局提出注册申请，经审查核准注册后，才能获得商标权。文学艺术作品和计算机软件等的著作权虽然是自作品完成其权利即自动产生，但有些国家也要实行登记或标注版权标记后才能得到保护。我国著作权法第二条规定“中国公民、法人或其他组织的作品，不论是否发表，依照本法享有著作权”。

试题 4 答案

(4) C

试题 5 分析

计算机软件著作权的客体是指著作权法保护的计算机软件著作权的范围（受保护的客体）。根据《著作权法》第三条和《计算机软件保护条例》第二条的规定，著作权法保护的计算机软件是指计算机程序及其有关文档。

计算机程序：根据《计算机软件保护条例》第三条第一款的规定，计算机程序是指为了得到某种结果而可以由计算机等具有信息处理能力的装置执行的代码化指令序列，或者可被自动转换成代码化指令序列的符号化语句序列。计算机程序包括源程序和目标程序，同一程序的源程序文本和目标程序文本视为同一软件作品。

计算机软件的文档：根据《计算机软件保护条例》第三条第二款的规定，计算机程序的文档是指用自然语言或者形式化语言所编写的文字资料和图表，以用来描述程序的内容、组成、设计、功能规格、开发情况、测试结果及使用方法等。文档一般以程序设计说明书、流程图、用户手册等形式表现。

试题 5 答案

(5) B

4.3 标准化法

在标准化法这个考点中，主要考查的是标准化这方面的内容。

4.3.1 考点精讲

标准化工作的任务是制定标准、组织实施标准和对标准的实施进行监督。

1. 标准的制定

在本节中，我们主要介绍标准的层次、标准的类型和标准的周期。

(1) 标准的层次

标准可以分为国际标准、国家标准、行业标准、地方标准和企业标准。

国际标准主要是指由国际标准化组织（International Standard Organization, ISO）制定和批准的标准。

国家标准由国务院标准化行政主管部门编制计划，组织草拟，统一审批、编号、发布。

对没有国家标准而又需要在全国某个行业范围内统一的技术要求，可以制定行业标准

(含标准样品的制作)。制定行业标准的项目由国务院有关行政主管部门确定。行业标准由国务院有关行政主管部门编制计划,组织草拟,统一审批、编号、发布,并报国务院标准化行政主管部门备案。行业标准在相应的国家标准实施后,自行废止。

对没有国家标准和行业标准而又需要在省、自治区、直辖市范围内统一的工业产品的安全、卫生要求,可以制定地方标准。制定地方标准的项目,由省、自治区、直辖市人民政府标准化行政主管部门确定。地方标准由省、自治区、直辖市人民政府标准化行政主管部门编制计划,组织草拟,统一审批、编号、发布,并报国务院标准化行政主管部门和国务院有关行政主管部门备案。法律对地方标准的制定另有规定的,依照法律的规定执行。地方标准在相应的国家标准或行业标准实施后,自行废止。

企业生产的产品没有国家标准、行业标准和地方标准的,应当制定相应的企业标准,作为组织生产的依据。企业标准由企业组织制定,并按省、自治区、直辖市人民政府的规定备案。对已有国家标准、行业标准或者地方标准的,鼓励企业制定严于国家标准、行业标准或者地方标准要求的企业标准,在企业内部适用。

(2) 标准的类型

国家标准、行业标准分为强制性标准和推荐性标准。下列标准属于强制性标准。

- ① 药品标准,食品卫生标准,兽药标准。
- ② 产品及产品生产、储运和使用中的安全、卫生标准,劳动安全、卫生标准,运输安全标准。
- ③ 工程建设的质量、安全、卫生标准及国家需要控制的其他工程建设标准。
- ④ 环境保护的污染物排放标准和环境质量标准。
- ⑤ 重要的通用技术术语、符号、代号和制图方法。
- ⑥ 通用的试验、检验方法标准。
- ⑦ 互换配合标准。
- ⑧ 国家需要控制的重要产品质量标准。

国家需要控制的重要产品目录由国务院标准化行政主管部门会同国务院有关行政主管部门确定。

强制性标准以外的标准是推荐性标准。省、自治区、直辖市人民政府标准化行政主管部门制定的工业产品的安全、卫生要求的地方标准,在本行政区域内是强制性标准。

(3) 标准的周期

标准实施后,制定标准的部门应当根据科学技术的发展和经济建设的需要适时进行复审。标准复审周期一般不超过5年。国家标准、行业标准和地方标准的代号、编号办法,由国务院标准化行政主管部门统一规定。企业标准的代号、编号办法,由国务院标准化行政主管部门会同国务院有关行政主管部门规定。标准的出版、发行办法,由制定标准的部门规定。

2. 标准的表示

按照新的国际标准管理办法,我国标准与国际标准的对应关系有等同采用(Identical, idt)、修改采用(Modified, mod)、等效采用(Equivalent, eqv)和非等效采用(Not Equivalent, neq)4种。

等同采用是指技术内容相同,没有或仅有编辑性修改,编写方法完全相对应。

等效采用(修改采用)是指主要技术内容相同,技术上只有很少差异,编写方法不完全

相对应。

非等效采用指与相应国际标准在技术内容和文本结构上不同，它们之间的差异没有被清楚地标明。非等效采用还包括在我国标准中只保留了少量或者不重要的国际标准条款的情况。非等效采用不属于采用国际标准。

推荐性标准的代号是在强制性标准代号后面加“/T”。国家标准代号如表 4-1 所示。

表 4-1 国家标准代号

序 号	代 号	含 义	管 理 部 门
1	GB	中华人民共和国强制性国家标准	国家标准化管理委员会
2	GB/T	中华人民共和国推荐性国家标准	国家标准化管理委员会
3	GB/Z	中华人民共和国国家标准化指导性技术文件	国家标准化管理委员会

与 IT 行业相关的各行业标准代号如表 4-2 所示。

表 4-2 行业标准代号

序 号	代 号	行 业	管 理 部 门
5	CY	新闻出版	国家新闻出版总署印刷业管理司
6	DA	档案	国家档案局政法司
8	DL	电力	中国电力企业联合会标准化中心
12	GA	公共安全	公安部科技司
13	GY	广播电影电视	国家广播电影电视总局科技司
14	HB	航空	国防科工委中国航空工业总公司（航空）
16	HJ	环境保护	国家环境保护总局科技标准司
19	JB	机械	中国机械工业联合会
20	JC	建材	中国建筑材料工业协会质量部
21	JG	建筑业	建设部（建筑业）
26	LD	劳动和劳动安全	劳动和社会保障部劳动工资司（工资定额）
39	SJ	电子	信息产业部科技司（电子）
48	WH	文化	文化部科教司
49	WJ	兵工民品	国防科工委中国兵器工业总公司（兵器）
55	YD	通信	信息产业部科技司（邮电）
58	YZ	邮政	国家邮政局计划财务部

另外，国家军用标准的代号为 GJB。地方标准的代号由地方标准代号（DB）、地方标准发布顺序号、标准发布年代号（4 位数）3 部分组成。企业标准的代号由企业标准代号（Q）、标准发布顺序号和标准发布年代号（4 位数）组成。

4.3.2 一点一练

试题 1

由我国信息产业部批准发布，在信息产业部门范围内统一使用的标准，称为__（1）__。
（1） A. 地方标准 B. 部门标准 C. 行业标准 D. 企业标准

试题 2

已经发布实施的标准（包括已确认或修改补充的标准），经过实施一定时期后，对其内容再次审查，以确保其有效性、先进性和适用性，其周期一般不超过__（2）__年。
（2） A. 1 B. 3 C. 5 D. 7

试题 3

____(3)____确定标准体制和标准化管理体制，规定制定标准的对象与原则，以及实施标准的要求，明确违法行为的法律责任和处罚办法。

- (3) A. 标准化 B. 标准 C. 标准化法 D. 标准与标准化

试题 4

《计算机软件产品开发文件编制指南》(GB 8567-88)是____(4)____标准。

- (4) A. 强制性 B. 推荐性 C. 强制性行业 D. 推荐性行业

试题 5

标准化是一门综合性学科，其工作内容极为广泛，可渗透到各个领域。标准化工作的特征包括横向综合性、政策性和____(5)____。

- (5) A. 统一性 B. 灵活性 C. 先进性 D. 安全性

4.3.3 解析与答案

试题 1 分析

我国的国家标准由国务院标准化行政主管部门制定；行业标准由国务院有关行政主管部门制定；地方标准由省、自治区和直辖市标准化行政主管部门制定；企业标准由企业自己制定。而信息产业部属于国务院有关行政主管部门范畴，故由其批准发布的标准属于行业标准。

试题 1 答案

- (1) C

试题 2 分析

标准复审 (Review of Standard) 是指已经发布实施的现有标准 (包括已确认或修改补充的标准)，经过实施一定时期后，对其内容再次审查，以确保其有效性、先进性和适用性的过程。1988 年发布的《中华人民共和国标准化法实施条例》中规定，标准实施后的复审周期一般不超过 5 年。

试题 2 答案

- (2) C

试题 3 分析

本试题考查《标准化法》的主要内容。《标准化法》分为五章二十六条，其主要内容是确定了标准体制和标准化管理体制 (第一章)，规定了制定标准的对象与原则以及实施标准的要求 (第二章、第三章)，明确了违法行为的法律责任和处罚办法 (第四章)。

标准是对重复性事物和概念所做的统一规定。标准以科学、技术和实践经验的综合成果为基础，以获得最佳秩序和促进最佳社会效益为目的，经有关方面协商一致，由主管或公认机构批准，并以规则、指南或特性的文件形式发布，作为共同遵守的准则和依据。

标准化是在经济、技术、科学和管理等社会实践中，以改进产品、过程和服务的适用性，防止贸易壁垒，促进技术合作。促进最大社会效益为目的，对重复性事物和概念通过制定、发布和实施标准，达到统一，获得最佳秩序和社会效益的过程。

试题 3 答案

- (3) C

试题 4 分析

常见的标准代号如下。

- ① GB: 中国国家强制标准。

- ② GB/T: 中国推荐性国家标准。
- ③ GJB: 中国国家军用标准。
- ④ JB: 中国机械行业（含机械、电工及仪器仪表等）强制性行业标准。
- ⑤ ISO: 国际标准化组织标准。
- ⑥ NAS: 美国国家航空航天标准。

试题 4 答案

(4) A

试题 5 分析

标准化工作的特征包括横向综合性、政策性、统一性。

试题 5 答案

(5) A

4.4 考前冲刺

试题 1

依据我国著作权法的规定，____(1)____属于著作人身权。

- (1) A. 发行权
- B. 复制权
- C. 署名权
- D. 信息网络传播权

试题 2

李某在《电脑知识与技术》杂志上看到张某发表的一组程序，颇为欣赏，就复印了 100 份作为程序设计辅导材料发给了学生。李某又将这组程序逐段加以评析，写成评论文章后投到 www.csai.cn 网站上发表。李某的行为____(2)____。

- (2) A. 侵犯了张某的著作权，因为其未经许可，擅自复印张某的程序
- B. 侵犯了张某的著作权，因为在评论文章中全文引用了发表的程序
- C. 不侵犯张某的著作权，其行为属于合理使用
- D. 侵犯了张某的著作权，因为其擅自复印，又在其发表的文章中全文引用了张某的程序

试题 3

关于软件著作权产生的时间，表述正确的是____(3)____。

- (3) A. 自作品首次公开发表时
- B. 自作者有创作意图时
- C. 自作品得到国家著作权行政管理部门认可时
- D. 自作品完成创作之日

试题 4

软件权利人与被许可方签订一份软件使用许可合同。若在该合同约定的时间和地域范围内，软件权利人不得再许可任何第三人以此相同的方法使用该项软件，但软件权利人可以自己使用，则该项许可使用是____(4)____。

- (4) A. 独家许可使用
- B. 独占许可使用
- C. 普通许可使用
- D. 部分许可使用

试题 5

利用____(5)____可以对软件的技术信息、经营信息提供保护。

- (5) A. 著作权
- B. 专利权
- C. 商业秘密权
- D. 商标权

试题 6

下列关于软件著作权中翻译权的叙述不正确的是：翻译权是指____(6)____的权利。

- (6) A. 将原软件从一种自然语言文字转换成另一种自然语言文字
- B. 将原软件从一种程序设计语言转换成另一种程序设计语言
- C. 软件著作权人对其软件享有的以其他各种语言文字形式再表现
- D. 对软件的操作界面或者程序中涉及的语言文字翻译成另一种语言文字

试题 7

____(7)____指可以不经著作权人许可，无须支付报酬，使用其作品。

- (7) A. 合理使用 B. 许可使用 C. 强制许可使用 D. 法定许可使用

试题 8

中国企业 M 与美国公司 L 进行技术合作，合同约定 M 使用一项在有效期内的美国专利，但该项美国专利未在中国和其他国家提出申请。对于 M 销售依照该专利生产的产品，以下叙述正确的是____(8)____。

- (8) A. 在中国销售，M 需要向 L 支付专利许可使用费
- B. 返销美国，M 不需要向 L 支付专利许可使用费
- C. 在其他国家销售，M 需要向 L 支付专利许可使用费
- D. 在中国销售，M 不需要向 L 支付专利许可使用费

试题 9

我国法律规定，计算机软件著作权的权利自软件开发完成之日起产生，对公民著作权的保护期限是____(9)____。

- (9) A. 作者有生之年加死后 50 年 B. 作品完成后 50 年
- C. 没有限制 D. 作者有生之年

试题 10

知识产权可分为两类，即____(10)____。

- (10) A. 著作权和使用权 B. 出版权和获得报酬权
- C. 使用权和获得报酬权 D. 工业产权和著作权

4.5 习题解析

试题 1 分析

著作权法规定：“著作权人可以全部或者部分转让本条第一款第（五）项至第（十七）项规定的权利，并依照约定或者本法有关规定获得报酬。”其中，包括署名权。

试题 1 答案

- (1) C

试题 2 分析

《中华人民共和国著作权法》第十二条规定：“改编、翻译、注释、整理已有作品而产生的作品，其著作权由改编、翻译、注释、整理人享有，但行使著作权时，不得侵犯原作品的著作权。”根据一件已有的作品，利用改编、翻译、注释、整理等演绎方式而创作的派生作品称之为演绎作品。演绎是一种创作，因而演绎作品是一种新创作的作品。演绎作者对其演绎作品享有完整的著作权。本题中李某将《电脑与编程》杂志上看到张某发表的一组程序逐段加以评析，写成评论文章后投到《电脑编程技巧》杂志上发表，故李某的“评论文章”属于演绎作品，其行为不侵犯张某的著作权，其行为属于合理使用。

试题 2 答案

(2) C

试题 3 分析

本题考查知识产权中关于软件著作权方面的知识。

在我国，软件著作权采用“自动保护”原则。《计算机软件保护条例》第十四条规定：“软件著作权自软件开发完成之日起产生。”即软件著作权自软件开发完成之日起自动产生，不论整体还是局部，只要具备了软件的属性即产生软件著作权，既不要求履行任何形式的登记或注册手续，也无须在复制件上加注著作权标记，也不论其是否已经发表都依法享有软件著作权。

一般来讲，一个软件只有开发完成并固定下来才能享有软件著作权。如果一个软件一直处于开发状态中，其最终的形态并没有固定下来，则法律无法对其进行保护。因此，条例（法律）明确规定软件著作权自软件开发完成之日起产生。当然，现在的软件开发经常是一项系统工程，一个软件可能会有很多模块，而每一个模块能够独立完成某一项功能。自该模块开发完成后就产生了著作权。所以说，自该软件开发完成后就产生了著作权。

试题 3 答案

(3) D

试题 4 分析

软件许可使用一般有独占许可使用、独家许可使用和普通许可使用三种形式。独占许可使用，许可的是专有使用权。实施独占许可使用后，软件著作权人不得将软件使用权授予第三方，软件著作权人不能使用该软件；独家许可使用，许可的是专有使用权，实施独家许可使用后，软件著作权人不得将软件使用权授予第三方，软件著作权人自己可以使用该软件；普通许可使用，许可的是非专有使用权，实施普通许可使用后，软件著作权人可以将软件使用权授予第三方，软件著作权人自己可以使用该软件。

试题 4 答案

(4) A

试题 5 分析

本题考查知识产权方面的基础知识，涉及软件商业秘密权的相关概念。

著作权从软件作品性的角度保护其表现形式，源代码（程序）、目标代码（程序）、软件文档是计算机软件的基本表达方式（表现形式），受著作权保护；专利权从软件功能性的角度保护软件的思想内涵，即软件的技术构思、程序的逻辑和算法等的思想内涵，当计算机软件同硬件设备是一个整体，涉及计算机程序的发明专利，可以申请方法专利，取得专利权保护；商标权是为商业化的软件从商品、商誉的角度为软件提供保护，利用商标权可以禁止他人使用相同或者近似的商标，生产（制作）或销售假冒软件产品，商标权受保护的力度大于其他知识产权，对软件的侵权行为更容易受到行政查处。而商业秘密权是商业秘密的合法控制人采取了保密措施，依法对其经营信息和技术信息享有的专有使用权，我国《反不正当竞争法》中对商业秘密的定义为“不为公众所知悉、能为权利人带来经济利益、具有实用性并经权利人采取保密措施的技术信息和经营信息”。软件技术秘密是指软件中适用的技术情报、数据或知识等，包括程序、设计方法、技术方案、功能规划、开发情况、测试结果及使用方法的文字资料和图表，如程序设计说明书、流程图、用户手册等。软件经营秘密指具有软件秘密性质的经营管理方法以及与经营管理方法密切相关的信息和情报，其中包括管理方法、经营方法、产销策略、客户情报（客户名单、客户需求），以及对软件市场的分析、预测报告和未来的发展规划、招投标中的标底及标书内容等。

试题 5 答案

(5) C

试题 6 分析

软件著作权中翻译权属于软件著作财产权，是指将原软件从一种自然语言文字转换成另一种自然语言文字的权利，而不是指将原软件从一种程序设计语言转换成另一种程序设计语言。

试题 6 答案

(6) B

试题 7 分析

合理使用是指可以不经著作权人许可，不需支付报酬，使用其作品；许可使用是指在获得著作权人许可后使用其作品；强制许可使用也称为强制许可或非自愿许可，是指国务院专利行政部门依照法律规定，可以不经专利权人的同意，直接允许申请人实施专利权人的发明或实用新型专利的一种行政措施；法定许可使用是指法律明文规定，可以不经著作权人许可，以特定的方式有偿使用他人已经发表的作品行为，并且这种使用应当尊重著作权人的其他各项人身权利和财产权。

试题 7 答案

(7) A

试题 8 分析

中国企业 M 与美国公司 L 进行技术合作，合同约定 M 使用一项在有效期内的美国专利，但该项美国专利未在中国和其他国家提出申请。对于 M 销售依照该专利生产的产品在中国销售，M 不需要向 L 支付专利许可使用费。

试题 8 答案

(8) D

试题 9 分析

本题考查知识产权保护方面的基本知识。

根据《中华人民共和国著作权法》和《计算机软件保护条例》的规定，计算机软件著作权的权利自软件开发完成之日起产生，公民的软件著作权保护期为公民终生及其死亡之后 50 年；法人或其他组织的软件著作权保护期为 50 年。保护期满，除开发者身份权以外，其他权利终止。一旦计算机软件著作权超出保护期后，软件进入公有领域。计算机软件著作权人的单位终止和计算机软件著作权人的公民死亡均无合法继承人的，除开发者身份权以外，该软件的其他权利进入公有领域。软件进入公有领域后成为社会公共财富，公众可无偿使用。

试题 9 答案

(9) A

试题 10 分析

本题考查知识产权方面的基本知识。我国知识产权法规定，知识产权可分为工业产权和著作权两类。

试题 10 答案

(10) D

网络体系结构

网络体系结构定义计算机设备和其他设备如何连接在一起以形成一个允许用户共享信息和资源的通信系统。存在专用网络体系结构，如 IBM 的系统网络系统结构（SNA）和 DEC 的数字网络体系结构（DNA），也存在开放体系结构，如国际标准化组织（ISO）定义的开放式系统互联（OSI）模型。

5.1 考点脉络

网络体系结构是网络工程师考试的一个考点，也是学习后续章节的基础。

根据考试大纲，要求考生掌握以下几个方面的内容。

- （1）OSI 参考模型与各层数据封装：包括 7 层名称与作用。
- （2）TCP/IP 协议栈：包括 TCP/IP 协议栈介绍、TCP/IP 协议栈和 OSI 模型的异同。
- （3）各层协议：包括 IP 协议、TCP 协议、UDP 协议、底层协议、高层协议等。

从历年的考试试题来看，本章的考点在综合知识考试中的平均分数为 3.6 分，约为总分的 5%。考试试题分数主要集中在 OSI 和 TCP/IP 协议栈的层次、TCP/UDP、底层协议、高层协议这 4 个知识点上。

5.2 参考模型

在参考模型这个考点中，主要涉及 OSI 参考模型和 TCP/IP 协议栈两个方面的内容。

5.2.1 考点精讲

OSI（Open System Interconnect）开放式系统互联。又称为 OSI 参考模型，是 ISO（国际标准化组织）组织在 1985 年研究的网络互联模型。该体系结构标准定义了网络互连的七层框架，即 ISO 开放系统互连参考模型。在这一框架下进一步详细规定了每一层的功能，以实现开放系统环境中的互连性、互操作性和应用的可移植性。

TCP/IP 协议叫做传输控制/网际协议，它是 Internet 国际互联网络的基础。TCP/IP 是网络中使用的基本的通信协议。

1. OSI 参考模型

对于本知识点的考查，关键在于各层结构特点、封装特性，代表性协议及其关键特性，主要是记忆型与理解型题目。

（1）七层结构

网络体系结构指的是网络各层、层中协议和层间接口的集合。OSI 网络体系结构中共定义了七层，从高到低分别介绍如下。

- ① 应用层：直接为端用户服务，提供各类应用过程的接口和用户接口。诸如 HTTP、Telnet、FTP、SMTP、NFS 等。
- ② 表示层：使应用层可以根据其服务解释数据的含义，通常包括数据编码的约定、本地句法的转换。诸如 JPEG、ASCII、GIF、DES、MPEG 等。
- ③ 会话层：主要负责管理远程用户或进程间的通信，通常包括通信控制、检查点设置、重建中断的传输链路、名字查找和安全验证服务。诸如 RPC、SQL、NFS 等。
- ④ 传输层：实现发送端和接收端的端到端的数据分组（数据段）传送，负责保证实现数据包无差错、按顺序、无丢失和无冗余的传输。其服务访问点为端口。代表性协议有 TCP、UDP、SPX 等。
- ⑤ 网络层：属于通信子网，通过网络连接交换传输层实体发出的数据（以报文分组的形式）。它解决的问题是路由选择、网络拥塞、异构网络互联的问题。其服务访问点为逻辑地址（也称为网络地址，通常由网络号和主机地址两部分组成）。代表性协议有 IP、IPX 等。
- ⑥ 数据链路层：简称数链层，建立、维持和释放网络实体之间的数据链路，这种数据链路对网络层表现为一条无差错的信道（传送数据帧）。它通常把流量控制和差错控制合并在一起。数据链路层可以分为 MAC（媒介访问层）和 LLC（逻辑链路层）两个子层，其服务访问点为物理地址（也称为 MAC 地址）。代表性协议有 IEEE 802.3/2、HDLC、PPP、ATM 等。
- ⑦ 物理层：通过一系列协议定义了通信设备的机械的、电气的、功能的、规程的特征。代表性协议有 RS-232、V.35、RJ-45、FDDI 等。物理层的数据将以比特流的形式进行传输。

OSI 模型各层实现的主要功能如表 5-1 所示。

表 5-1 OSI 各层功能分布

层 次	主 要 功 能
物理层	提供物理通路、二进制数据传输、定义机械/电气特性和接口
数链层	数据链路的链接与释放、流量控制、构成链路数据单元、差错的检测与恢复、帧定界与同步、传送以帧为单位的信息
网络层	路由的选择与中继、网络连接的激活与终止、网络连接的多路复用、差错的检测与恢复、排序与流量控制、服务选择
传输层	映射传输地址到网络地址、传输连接的建立与释放、多路复用与分割、差错控制及恢复、分段与重组、组块与分块、序号及流量控制
会话层	会话链接到传输链接映射、会话链接的恢复与释放、对会话参数进行协商 服务选择、活动管理与令牌管理、数据传送
表示层	数据语法的转换、数据加密与数据压缩、语法表示与连接管理
应用层	应用层包含用户应用程序执行任务所需要的协议和功能

OSI 体系结构方面规定了开放系统在分层、相应层对等实体的通信、标识符、服务访问点、数据单元、层操作、OSI 管理等方面的基本元素、组成和功能等，如表 5-2 所示。

表 5-2 数据封装

层 次	物理层	数链层	网络层	传输层	会话层	表示层	应用层
封 装 单 位	比特流	数据帧	数据包	信息报文			

（2）服务访问点

（N）层实体向（N+1）层实体提供服务，（N+1）层实体向（N）层实体请求服务，从概念上讲，这是通过位于（N）层和（N+1）层的界面上的服务访问点（N）SAP 来实现的，

如图 5-1 所示。

(N) SAP 是一个访问工具，由一组服务元素和抽象操作组成，并由 (N+1) 实体在该点调用。我们把 (N) 层中提供 (N) 服务的那些 (N) 实体总称为 (N) 服务提供者；而把调用 (N) 服务的 (N+1) 实体称为 (N) 服务用户。

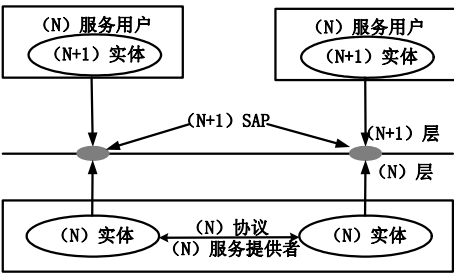


图 5-1 服务访问点 SAP

这里要掌握的是：MAC 地址是物理层的 SAP，为数据链路层服务；LLC 地址是逻辑链路层的 SAP；IP 地址是网络层的 SAP，为传输层提供服务；端口号是传输层上的 SAP，为上层应用提供服务；用户界面是应用层的 SAP，为主体用户提供服务。

2. TCP/IP 协议族

1983 年 1 月 1 日，互联网的前身 Arpanet 中，TCP/IP 协议取代了旧的网络核心协议 NCP (Network Core Protocol)，从而成为今天的互联网的基石。最早的 TCP/IP 由 Vinton Cerf 和 Robert Kahn 两人开发，慢慢地通过竞争战胜了其他一些网络协议的方案，比如国际标准化组织 ISO 的 OSI 模型。TCP/IP 的蓬勃发展发生在 20 世纪的 90 年代中期。

TCP/IP 协议族也是一种层次体系结构，共分为 4 层，如图 5-2 所示。

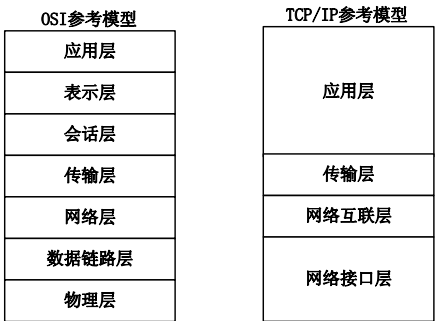


图 5-2 TCP/IP 协议与 OSI 分层对比

其中的底层物理层和数据链路层只要能够支持 IP 层的分组传送即可，因此作为网络接口层来对待，如图 5-3 所示。

各层的功能简介如下。

(1) 网络接口层：提供 IP 数据报的发送和接收。例如，以太网的 802.3 协议、令牌环网的 802.5 协议以及分组交互网的 X.25 协议等。

(2) 网络互联层：提供计算机间的分组传输。

主要体现在高层数据的分组生成、底层数据报的分组组装、处理路由、流控、拥塞等方面。

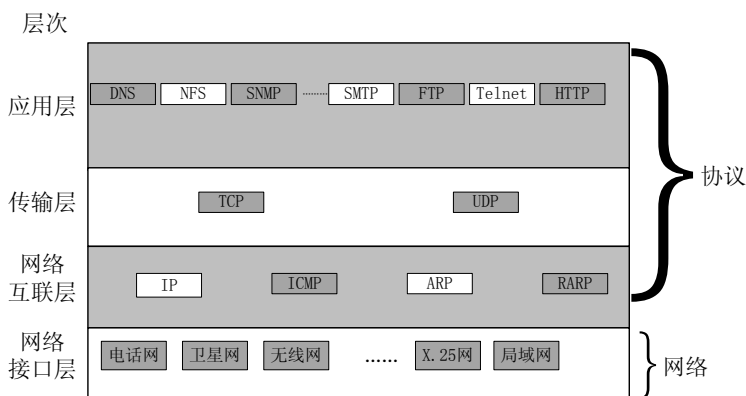


图 5-3 TCP/IP 模型

(3) 传输层：提供应用程序间的通信、格式化信息流、提供可靠传输。

TCP 协议提供面向连接的可靠的字节流传输，UDP 协议提供无连接的不可靠的数据包传输。

(4) 应用层：提供常用的应用程序。例如，WWW 服务、FTP、E-mail、Telnet 等。

5.2.2 一点一练

试题 1

在 OSI 参考模型中，上层协议实体与下层协议实体之间的逻辑接口叫做服务访问点 (SAP)。在 Internet 中，网络层的服务访问点是 (1)。

- (1) A. MAC 地址 B. LLC 地址 C. IP 地址 D. 端口号

试题 2

在 OSI 参考模型中，实现端到端的应答、分组排序和流量控制功能的协议层是 (2)。

- (2) A. 数据链路层 B. 网络层 C. 传输层 D. 会话层

试题 3

在 ISO OSI/RM 中， (3) 实现数据压缩功能。

- (3) A. 应用层 B. 表示层 C. 会话层 D. 网络层

试题 4

以太网中的帧属于 (4) 协议数据单元。

- (4) A. 物理层 B. 数据链路层 C. 网络层 D. 应用层

试题 5

在 TCP/IP 体系结构中，BGP 协议是一种 (5)，BGP 报文封装在 (6) 中传送。

- (5) A. 网络应用 B. 地址转换协议 C. 路由协议 D. 名字服务
(6) A. 以太帧 B. IP 数据包 C. UDP 报文 D. TCP 报文

5.2.3 解析与答案

试题 1 分析

此题引用了 ISO OSI/RM 的服务访问点的概念，但问的却是 TCP/IP 参考模型的知识，因为 Internet 使用的是 TCP/IP 协议。

在 TCP/IP 参考模型中，网络接口层的 SAP 是 MAC 地址。在网络层（也可称为网络层）使用的协议主要是 IP 协议，其 SAP 便是 IP 地址；而传输层使用的主要协议为 TCP 和 UDP，

TCP 使用的 SAP 为 TCP 的端口号，UDP 使用的 SAP 为 UDP 的端口号。

试题 1 答案

(1) C

试题 2 分析

此题主要考查了 ISO OSI/RM 体系结构中各层的主要功能。

物理层：物理层主要是设计处理机械的、电气的和过程的接口，以及物理层下的物理传输介质等问题。

数据链路层：负责在两个相邻节点间的线路上，无差错地传送以帧（Frame）为单位的数据以及流量控制信息，即差错控制、流量控制、帧同步。

网络层：主要是确定数据报（Packet）从发送方到接收方应该如何选择路由，以及拥塞控制、数据报的分片与重组。

传输层：负责两个端节点之间的可靠网络通信和流量控制，即面向连接的通信、端到端的流量控制、差错控制。

会话层：建立、管理和终止应用程序会话和管理表示层实体之间的数据交换。

表示层：翻译、加/解密、压缩和解压。

应用层：提供了大量容易理解的协议，允许访问网络资源。

试题 2 答案

(2) C

试题 3 分析

ISO OSI/RM 7 个协议层的功能可以概括描述如下。

物理层：规定了网络设备之间的物理连接的标准，在网络设备之间透明地传输比特流。

数据链路层：在通信子网中进行路由选择和通信控制。

网络层：主要是确定数据报（Packet）从发送方到接收方应该如何选择路由，以及拥塞控制、数据报的分片与重组。

传输层：提供两个端系统之间的可靠通信。

会话层：建立和控制两个应用实体之间的会话过程。

表示层：提供统一的网络数据表示。

应用层：提供两个网络用户之间的分布式应用环境（普通用户）和应用开发环境（高级用户，即网络程序员）。

这样的描述虽然没有穷尽各个协议层的功能细节，但是表达了各个协议层的主要功能。当然 ISO 对各个协议层的功能也进行了扩充，但是以上所述是 OSI/RM 各个协议层最原始和最重要的功能。由于数据压缩属于数据表示的范畴，所以应归于表示层。

试题 3 答案

(3) B

试题 4 分析

局域网只有物理层和数据链路层。物理层规定了传输介质及其接口的机械特性、电气特性、接口电路的功能以及信令方式和数据速率等。IEEE 802 标准把数据链路层划分为两个子层。与物理介质无关的部分叫做逻辑链路控制 LLC（Logical Link Control）子层，与物理介质相关的部分叫做介质访问控制 MAC（Media Access Control）子层。所以局域网的数据链路层有两种不同的协议数据单元：LLC 帧和 MAC 帧。从高层来的数据加上 LLC 的帧头就称为 LLC 帧，再向下传送到 MAC 子层，加上 MAC 的帧头和帧尾，组成 MAC 帧。物理层则把 MAC 帧当作比特流透明地在数据链路实体间传送。虽然 LLC 标准只有一个（由 IEEE

802.2 定义, 与 HDLC 兼容), 但是支持它的 MAC 标准却有多, 并且都是与具体的传输介质和拓扑结构相关的。

以太帧属于 MAC 子层, 是 MAC 层的协议数据单元。另外其他局域网 (例如令牌环网或令牌总线网) 的协议数据单元也属于 MAC 帧。

试题 4 答案

(4) B

试题 5 分析

BGP 协议是一种路由协议, 叫做边界网关协议 (Border Gateway Protocol), 运行在不同自治系统的路由器之间。BGP 报文通过 TCP 连接传送, 这是因为边界网关之间不仅需要身份认证, 还要可靠地交换路由信息, 所以使用了面向连接的网络服务。

试题 5 答案

(5) C

(6) D

5.3 各种协议

在各种协议这个考点中, 主要涉及传输层 TCP/UDP 协议、网络层 IP 协议、其他低层协议和高层协议 4 个方面的内容。

5.3.1 考点精讲

传输层两个非常重要的协议是 TCP 和 UDP。TCP 协议是可靠有连接服务, UDP 是不可靠无连接服务, 二者都有其不同的应用场合。

IP 是网络层核心协议, 本章节主要是介绍了 IP 封装, 后续章节还有 IP 寻址和 IP 规划的内容。

TCP/IP 协议栈也有 5 层划分法, 对应的层次分别是物理层、数据链路层、网络层、传输层、应用层。人们常提到的低层协议指的是 TCP/IP 协议栈下三层协议 (物理层、数据链路层、网络层协议), 而高层协议更多指的是 TCP/IP 协议栈应用层的协议。

1. TCP 与 UDP

对于本知识点的考查, 主要是传输层 TCP/UDP 的一些传输特性、数据格式, 以及各自支持的应用层协议等知识。

(1) UDP 协议

UDP 即用户数据报协议, 是一个无连接服务的协议。它提供多路复用和差错检测功能, 但不保证数据的正确传送和重复出现。UDP 报头包括 16 位的源和目的端口号, 16 位的以字节为单位的长度总和 (数据和报头的和) 标识字段, 16 位的数据和报头校验和字段。

基于 UDP 的应用层协议有 SNMP、DNS、TFTP、DHCP、RPC 等。

(2) TCP 协议

TCP 即传输控制协议, 是一个面向连接的协议, 它提供双向的、可靠的、有流量控制的字节流的服务。字节流服务的意思是, 在一个 TCP 连接中, 源节点发送一连串的字节的节点。可靠服务是指数据有保证地传递、按序、没有重复。TCP 报头格式如图 5-4 所示。

TCP 协议是一种面向连接的、可靠的传输层协议。面向连接是指一次正常的 TCP 传输需要通过在 TCP 客户端和 TCP 服务端建立特定的虚电路连接来完成, 该过程通常被称为“三次握手”。三次握手的目标是使数据段的发送和接收同步, 同时也向其他主机表明其一次可接收的数据量 (窗口大小), 并建立逻辑连接。这三次握手的过程可以简述如下:



图 5-4 TCP 报头格式

源主机发送一个同步标志位(SYN)置 1 的 TCP 数据段。此段中同时标明初始序号(Initial Sequence Number, ISN)，ISN 是一个随时间变化的随机值。

目标主机发回确认数据段，此段中的同步标志位 (SYN) 同样被置 1，且确认标志位 (ACK) 也置 1，同时确认序号字段表明目标主机期待收到源主机下一个数据段的序号 (即表明前一个数据段已收到并且没有错误)。此外，此段中还包含目标主机的段初始序号。

源主机再回送一个数据段，同样带有递增的发送序号和确认序号。

至此，TCP 会话的三次握手完成。接下来，源主机和目标主机可以互相收发数据。

基于 TCP 的应用层协议有 SMTP、FTP、HTTP、Telnet、POP 等。

2. IP 协议

IP 协议实际上是一套由软件程序组成的协议软件，它把各种不同“帧”统一转换成“IP 数据报”格式，这种转换是因特网的一个最重要的特点，使所有各种计算机都能因在因特网上实现互通，即具有“开放性”的特点。

数据报也是分组交换的一种形式，就是把所传送的数据分段打成“包”，再传送出去。但是，与传统的“连接型”分组交换不同，它属于“无连接型”，是把打成的每个“包”(分组)都作为一个“独立的报文”传送出去，所以叫做“数据报”。这样，在开始通信之前就不需要先连接好一条电路，各个数据报不一定都通过同一条路径传输，所以叫做“无连接型”。这一特点非常重要，它大大提高了网络的坚固性和安全性。

每个数据报都有包头和包文两个部分，包头中有目的地址等必要内容，使每个数据报不经过同样的路径都能准确地到达目的地。在目的地重新组合还原成原来发送的数据，这就要求 IP 具有分组打包和集合组装的功能。在实际传送过程中，数据报还要求能根据所经过网络规定的分组大小来改变数据报的长度，IP 数据报的最大长度可达 65 535 个字节。IPv4 包头格式如图 5-5 所示。

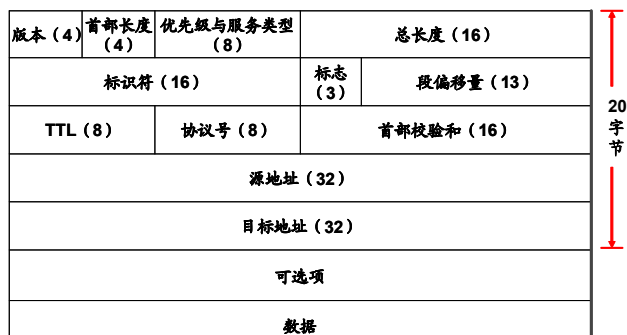


图 5-5 IPv4 包头格式

IP 协议运行在网络层上,可实现异构的网络之间的互联互通。它是一种不可靠、无连接的协议。IP 定义了在整个 TCP/IP 互联网上数据传输所用的基本单元(由于采用的是无连接的分组交换,因此也称为数据报),规定了互联网上传输数据的确切格式。IP 软件完成路由选择的功能,选择一个数据发送的路径。除了数据格式和路由选择精确而正式的定义之外,还包括一组不可靠分组传送思想的规则。这些规则指明了主机和路由器应该如何处理分组,何时采用何种方法发出错误信息,以及在什么情况下可以放弃分组。IP 协议是 TCP/IP 互联网设计中最基本的部分。对于 IP 协议而言,需要掌握以下几个关键知识点。

① 数据报生存期

为了防止因出现网络路由环路而导致 IP 数据报在网络中无休止地转发,IP 协议在 IP 包头设置了一个数据报生存期(TTL)位,用来存放数据报生存期(以跳为单位,每经过一个路由器为一跳),每经过一个路由器,计数器加 1,超过一定的计数值,就将其丢弃。

② 分段和重装配

在理想情况下,整个数据报被封装在一个物理帧中,可以提高物理网络上的效率。但由于 IP 数据报经常在许多类型的物理网络上传送,而每种物理网络所能够传送的帧的长度是有限的,例如以太网是 1500 字节,FDDI 是 4470 字节,这个限制称为网络最大传送单元(MTU)。这就使得 IP 协议在设计上不得不处理这样的矛盾:当数据报通过一个可传送更大帧的网络时,如果数据报大小限制为整个最小的 MTU,就会浪费网络带宽资源;但如果数据报大小大于最大的 MTU,就可能出现无法封装的问题。为了有效地解决这个问题,IP 协议采用了分段和重装配机制来解决。

a. 分段:IP 协议采用的是遇到 MTU 更小的网络时再分段。

b. 重装配:为了能够减少中途路由器的工作,降低出错率,重装配工作是直到目的主机时才进行的,也就是分段后,遇到 MTU 更大的网络时并不重装配,而是保持小分组,直到目的主机接收完整后再一次性重装配。

它使用了 4 个字段来处理分段和重装配问题,一是报文 ID 字段,它唯一标识了某个站某个协议层发出的数据;第二个字段是数据长度,即字节数;第三个字段是偏置值,即分段在原来数据报中的位置以 8 个字节的倍数计算;第四个是 M 标志,用来标识是否为最后一个分段。整个分段的步骤为如下。

a. 对数据块的分段必须在 64 位(8 字节)的边界上划分,因而除最后一段外,其他段长都是 64 位的整数倍。

b. 对得到的每一个分段都加上原来的数据报的 IP 头,组成短报文。

c. 每一个短报文的长度字段修改为它实际包含的字节数。

d. 第一个短报文的偏置值设置为 0,其他的偏置值为其前面所有报文长度之和除以 8。

e. 最后一个报文的 M 标志置为 0(False),其他报文的 M 标志置为 1(True)。

如图 5-6 所示就是一个“分段”的实例。

③ IP 数据报格式

IP 协议的数据报格式如图 5-5 所示,其中版本号用来说明 IP 协议的版本(现在是 IPv4,今后会过渡到 IPv6);IHL 是 IP 头长度(即除了用户数据之外),以 32 位字计数,最小是 5,即 20 个字节;服务类型用于区分可靠性、优先级、延迟和吞吐率的参数;总长度是包含 IP 头在内的数据单元总长度;标识符是唯一标识数据报的 ID;标志区有三个,一个未启用,D 代表是否允许分段,M 代表是否分段;协议表示使用的上层协议。

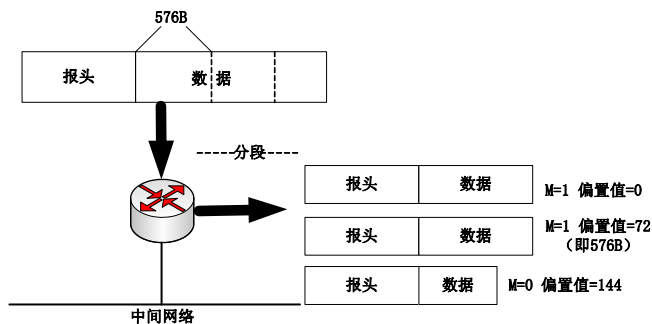


图 5-6 数据报分段示意图

3. 低层协议

本知识点的重点在于掌握 ARP/RARP、ICMP、HDLC 等协议的特性与应用。

(1) ARP 与 RARP

ARP 协议主要负责将局域网中的 32 位 IP 地址转换为对应的 48 位物理地址，即网卡的 MAC 地址，如 IP 地址为 192.168.0.1，网卡的 MAC 地址为 00-03-0F-FD-1D-2B。整个转换过程是一台主机先向目标主机发送包含 IP 地址信息的广播数据报，即 ARP 请求，然后目标主机向该主机发送一个含有 IP 地址和 MAC 地址的数据报，通过 MAC 地址，两个主机就可以实现数据传输了。

在安装了以太网网络适配器的计算机中有专门的 ARP 缓存，包含一个或多个表，用于保存 IP 地址以及经过解析的 MAC 地址。在 Windows 中要查看或者修改 ARP 缓存中的信息，可以使用 arp 命令来完成，例如在 Windows XP 的命令提示符窗口中，键入“arp -a”或“arp -g”可以查看 ARP 缓存中的内容；键入“arp -d IPaddress”表示删除指定的 IP 地址项(IPaddress 表示 IP 地址)。arp 命令的其他用法可以键入“arp /?”查看到。

RARP（反向地址转换协议）允许局域网的物理机器从网关服务器的 ARP 表或者缓存上请求其 IP 地址。网络管理员在局域网网关路由器里创建一个表以映射物理地址（MAC）和与其对应的 IP 地址。

(2) ICMP

ICMP 协议是 TCP/IP 协议集中的一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到 IP 数据无法访问目标、IP 路由器无法按当前的传输速率转发数据 q 包等情况时，会自动发送 ICMP 消息。我们可以通过 Ping 命令发送 ICMP 回应请求消息并记录收到 ICMP 回应回复消息，通过这些消息来对网络或主机的故障诊断提供参考依据。

ICMP 协议对于网络安全具有极其重要的意义。ICMP 协议本身的特点决定了它非常容易被用于攻击网络上的路由器和主机。例如，可以利用操作系统规定的 ICMP 数据报最大不超过 64KB 这一规定，向主机发起“Ping of Death”（死亡之 Ping）攻击。“Ping of Death”攻击的原理是：如果 ICMP 数据包的大小超过 64KB 上限时，主机就会出现内存分配错误，导致 TCP/IP 堆栈崩溃，致使主机死机。禁用 ICMP 所提供的相应端口，可以限制外来主机的 Ping 入。

ICMP 发送的消息类型主要有如下几种。

① 未达目的地信息

相应于网关的路由表，如果在目的域中指定的网络不可达，如网络距离为无限远，网关

会向发送源数据的主机发送目的不可达消息。而且，在一些网络中，网关有能力决定目的主机是否可达。如果目的地不可达，它将向发送源数据的主机发送不可达信息。

在目的主机，如果 IP 模块因为指定的协议模块和进程端口不可用而不能提交数据报，目的主机将向发送源数据的主机发送不可达信息。

另外一种情况是当数据报必须被分段传送，而“不可分段”位打开时，在这种情况下，网关必须抛弃此数据报，并向发送源数据的主机发送不可达信息。

② 超时信息

如果网关在处理数据报时发现生存周期域为零，此数据报必须抛弃。网关同时必须通过超时信息通知源主机。如果主机在组装分段的数据报时因为丢失段未能在规定时间内组装数据，此数据报必须抛弃，网关发送超时信息。

③ 参数问题消息

如果网关或主机在处理数据报时发现包头参数有错误以至不能完成工作，它必须抛弃此数据报。一个潜在的原因可能是变量的错误。网关或主机将通过参数问题消息通知源主机，此消息只有在消息被抛弃时才被发送。指针指向发现错误的数据报包头字节。

④ 源拥塞（抑制）消息

如果没有缓冲容纳，网关会抛弃数据报，如果网关这样做了，它会发送源拥塞消息给发送主机。如果接收的数据报太多无法处理，目的主机也会发送相应的消息给发送主机。此消息要求发送方降低发送速率，网关会给每个抛弃的消息返回源拥塞消息，在接收到此消息后，发送主机应该降低发送速率，直到不再接收到网关发送的源拥塞消息为止。在此之后，源主机可以再提高发送速率，直到接收到目的主机的源拥塞消息为止。网关或主机不会等到已经超过限度后再发送此消息，而是接近自己的处理极限时就发送此消息，这意味着，引发源拥塞消息的数据报仍然可以处理。

⑤ 重定向消息

网关在下面情况下发送重定向消息。网关（G1）从网关相连的网络上接收到数据报，它检查路由表获得下一个网关（G2）的地址（X）。如果 G2 和指定的接收主机在同一网络上，重定向消息发出，此消息建议发送主机直接将数据报发向网关 G2，因为这更近，同时网关 G1 向前继续发送此数据报。

因为在数据报中的 IP 源路由和目的地址域是可选的，所以即使有更好的路由有时也无法发现。

⑥ 回送或回送响应消息

回送消息中接收到的消息应该在回送响应消息中返回。标识符和序列码由回送发送者使用帮助匹配回送请求的响应。

⑦ 时间戳和时间戳响应消息

接收到的时间戳附加在响应里返回，时间是以百万分之一秒为单位计算的，并以标准时午夜开始计时。原时间戳是发送方发送前的时间。接收时间戳是回送者接收到的时间，传送时间是回送者发送的时间。

如果时间以百万分之一秒计算无效，或者不能以标准时提供，可以在时间戳的高字节填充数据以表示这不是标准数据。标识符和序列码由发送者匹配请求的响应。

⑧ 信息请求或信息响应消息

此消息可以在 IP 包头中以源网络地址发送，但同时目的地址域为 0（这表示此网络内）。

响应 IP 模块应该发送完全指定地址的响应。发送此消息是主机寻找到自己所在网络号码的一种方法。标识符和序列码由发送者匹配请求的响应。

(3) HDLC

HDLC 帧格式包括标志字段、地址字段、控制字段、数据和校验和，如图 5-7 所示。



图 5-7 HDLC 帧格式

标志字段（01111110）用于确定帧的起始和结束，以进行帧同步和准确识别长度可变的帧。

在两个标志字段之间的比特串中，如果碰巧出现了和标志字段一样的组合，就会被误认为是帧边界。为了避免这种错误，HDLC 采用比特填充法使一个帧中两个标志字段之间不会出现 6 个连续的 1。具体做法是：在发送端，在加标志字段之前，先对比特串扫描，若发现 5 个连续的 1，则立即在其后加一个 0。在接收端收到帧后，去掉头尾的标志字段，对比特串进行扫描，当发现 5 个连续的 1 时，立即删除其后的 0，这样就还原成原来的比特流了。

分组层 PLP (Packet Layer Procedure)
链路层 LAP和LAPB
物理层 X.21, 也可用RS232和V.35代替

图 5-8 X.25 规定的接口

(4) X.25

X.25 规定了主机 DTE 和网络设备 DCE 之间的三个层次上的接口，如图 5-8 所示。

① 物理层：相当于 OSI 参考模型的第一层。采用 X.21 物理接口，也可以选择类似于 RS-232C 的 X.21bis。

② 链路层：相当于 OSI 参考模型的第二层。采用 LAP 和 LAPB 链路访问规程，当 DTE 与 DCE 之间有多条并列物理电路时允许使用多链路规程（MLP）。

③ 分组层：相当于 OSI 参考模型的第三层。网络向主机提供多信道的虚电路业务，包括虚呼叫和永久虚电路业务。

4. 高层协议

本部分的知识点主要是对常见应用层协议以及相关知识的介绍，其中各协议经常轮换出题。

(1) 简单邮件传送协议

SMTP（简单邮件传送协议）决定了用户代理 MUA 与报文传送代理 MTA 建立连接的方法，以及 MUA 发送其电子邮件的方法。MTA 也使用 SMTP 在相互之间进行电子邮件的转发，直到电子邮件到达合适的 MTA 并传递给接收的 MUA。MUA 与 MTA，MTA 与 MTA 之间有着相类似的交互处理，其差别在于后者要求 MTA 必须查找一个接收 MTA。

(2) 邮局协议

SMTP 运行的前提是接收邮件的服务器端程序的目的主机一直在运行，否则就不能建立 TCP 连接，而这又不现实，因为桌面计算机每天要关机，不可能建立 SMTP 会话。TCP/IP 专门设计了一个提供对电子邮件信箱进行远程存取的协议，它允许用户的邮箱安置在某个运行邮件服务器程序的计算机（邮件服务器）上，并允许用户从其个人计算机对邮箱的内容进行存取。这个协议就是邮局协议 POP，现在用的是 POP3。

(3) 文件传送协议

在客户和服务器的文件传送过程中，有两个进程：控制进程和数据传送进程，同时工作。控制进程负责建立传送 FTP（文件传输协议）命令控制连接，这些命令使服务器知道要传送什么文件。控制进程即前面的子进程，客户端在向服务器发出连接请求时，还要告诉服务器自己的另一个端口号码，用于建立数据传送，数据进程用来建立数据连接，传送每个文件。服务器用自己的传送数据熟知端口（20）与客户端建立数据传送连接，如图 5-9 所示。

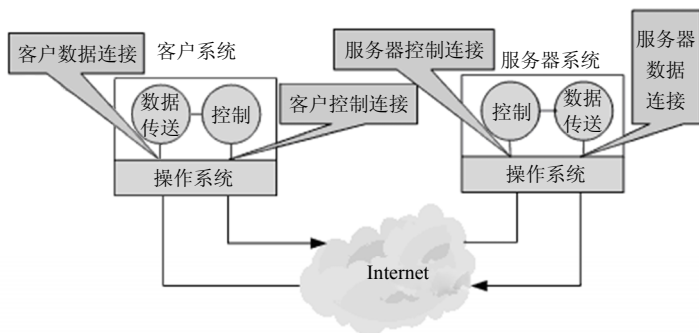


图 5-9 FTP 文件传输服务

(4) 普通文件传输协议

Internet 协议包括另外一个被称作普通文件传输协议 TFTP 的文件传输服务。TFTP 在多个方面与 FTP 存在着差异。

首先，TFTP 客户与服务器之间的通信使用的是 UDP 而非 TCP。其次，TFTP 只支持文件传输。也就是说，TFTP 不支持交互，而且没有一个庞大的命令集。最为重要的是，TFTP 不允许用户列出目录内容或者与服务器协商来决定那些可得到的文件名。第三，TFTP 没有授权。客户不需要发送登录名或者口令，文件仅当权限允许全局存取时才能被传输。

(5) 远程登录协议

远程登录协议 Telnet 是一个简单的远程终端协议，用户用 Telnet 可通过 TCP 登录到远地的一个主机上。Telnet 将用户的击键传到远地主机，也将远地主机的输出通过 TCP 连接返回到用户屏幕，使用户感觉到像是键盘和屏幕直接连到主机上一样。

Telnet 也使用客户/服务器模式，本地系统运行 Client 进程，远地主机则运行 Server 进程。和 FTP 一样，Server 中的主进程等待新的请求，并产生从属进程来处理每一个连接。

(6) WWW 与超文本传输协议

众所周知，Internet 的基本协议是 TCP/IP 协议，目前广泛采用的 FTP 等是建立在 TCP/IP 协议之上的应用层协议，不同的协议对应着不同的应用。WWW 服务器使用的主要协议是 HTTP 协议，即超文体传输协议。

HTTP 是一个属于应用层的面向对象的协议，由于其简捷、快速的方式，适用于分布式超媒体信息系统。HTTP 协议的主要特点可概括如下。

- 支持客户/服务器模式。
- 简单快速：客户向服务器请求服务时，只需传送请求方法和路径。常用的请求方法有 GET、HEAD、POST。每种方法规定了客户与服务器联系的类型不同。
- 灵活：HTTP 允许传输任意类型的数据对象。
- 无连接：无连接的含义是限制每次连接只处理一个请求。服务器处理完客户的请求，并收到客户的应答后，即断开连接。

- 无状态：HTTP 协议是无状态协议。无状态是指协议对于事务处理没有记忆能力。缺少状态意味着如果后续处理需要前面的信息，则它必须重传，这样可能导致每次连接传送的数据量增大。

(7) DNS 协议

域名系统（服务）协议（DNS）是一种分布式网络目录服务，主要用于域名与 IP 地址的相互转换，以及控制因特网的电子邮件的发送。大多数因特网服务依赖于 DNS 来工作，一旦 DNS 出错，就无法连接 Web 站点，电子邮件的发送也会中止。DNS 有如下两个独立的方面。

定义了命名语法和规范，以利于通过名称委派域名权限。基本语法是：local.group.site。

定义了如何实现一个分布式计算机系统，以便有效地将域名转换成 IP 地址。

在 DNS 命名方式中，采用了分散和分层的机制来实现域名空间的委派授权，以及域名与地址相转换的授权。通过使用 DNS 的命名方式来为遍布全球的网络设备分配域名，而这则是由分散在世界各地的服务器实现的。

理论上，DNS 协议中的域名标准阐述了一种可用任意标签值的分布式的抽象域名空间。任何组织都可以建立域名系统，为其所有分布结构选择标签，但大多数 DNS 协议用户遵循官方因特网域名系统使用的分级标签。常见的顶级域有：com、edu、gov、net、org，另外还有一些带国家和地区代码的顶级域如：cn、us、uk、hk 等。

DNS 的分布式机制支持有效且可靠的名字到 IP 地址的映射。多数名字可以在本地映射，不同站点的服务器相互合作能够解决大网络的名字与 IP 地址的映射问题。单个服务器的故障不会影响 DNS 的正确操作。DNS 是一种通用协议，它并不仅限于网络设备名称。

5.3.2 一点一练

试题 1

关于 HDLC 协议的帧顺序控制，下面的语句中正确的是____(1)____。

- (1) A. 如果接收器收到一个正确的信息帧 (I)，并且发送顺序号落在接收窗口内，则发回确认帧
- B. 信息帧 (I) 和管理帧 (S) 的控制字段都包含发送顺序号
- C. 如果信息帧 (I) 的控制字段是 8 位，则发送顺序号的取值范围是 0~127
- D. 发送器每发出一个信息帧 (I)，就把窗口向前滑动一格

试题 2

以下关于 X.25 网络的描述中，正确的是____(2)____。

- (2) A. X.25 的网络层提供无连接的服务
- B. X.25 网络丢失帧时，通过检查帧顺序号重传丢失帧
- C. X.25 网络使用 LAP-D 作为传输控制协议
- D. X.25 网络采用多路复用技术，帧中的各个时槽被预先分配给不同的终端

试题 3

下面语句中，正确地描述了网络通信控制机制的是____(3)____。

- (3) A. 在数据报系统中，发送方和接收方之间建立了虚拟通道，所有通信都省略了通路选择的开销
- B. 在滑动窗口协议中，窗口的滑动由确认的帧编号控制，所以可以连续发送多个帧
- C. 在前向纠错系统中，由接收方检测错误，并请求发送方重发出错帧

- D. 由于 TCP 协议的窗口大小是固定的, 无法防止拥塞出现, 所以需要超时机制来处理网络拥塞的问题

试题 4

关于无连接的通信, 下面的描述中正确的是____(4)_____。

- (4) A. 由于为每一个分组独立地建立和释放逻辑连接, 所以无连接的通信不适合传送大量的数据
B. 由于通信对方和通信线路都是预设的, 所以在通信过程中无须任何有关连接的操作
C. 目标的地址信息被加在每个发送的分组
D. 无连接的通信协议 UDP 不能运行在电路交换或租用专线网络上

试题 5

下面关于 ICMP 协议的描述中, 正确的是____(5)_____。

- (5) A. ICMP 协议根据 MAC 地址查找对应的 IP 地址
B. ICMP 协议把公网的 IP 地址转换为私网的 IP 地址
C. ICMP 协议根据网络通信的情况把控制报文传送给发送方主机
D. ICMP 协议集中管理网络中的 IP 地址分配

试题 6

下面信息中____(6)_____包含在 TCP 头中而不包含在 UDP 头中。

- (6) A. 目标端口号
B. 顺序号
C. 发送端口号
D. 校验和

试题 7

在 X.25 网络中, ____ (7) _____是网络层协议。

- (7) A. LAP-B B. X.21 C. X.25PLP D. MHS

试题 8

ARP 协议的作用是____(8)_____。

- (8) A. 由 IP 地址查找对应的 MAC 地址
B. 由 MAC 地址查找对应的 IP 地址
C. 由 IP 地址查找对应的端口号
D. 由 MAC 地址查找对应的端口号

试题 9

ARP 报文封装在____(9)_____中传送。

- (9) A. 以太网帧
B. IP 数据报
C. UDP 报文
D. TCP 报文

试题 10

简单邮件传输协议 (SMTP) 默认的端口号是____(10)_____。

- (10) A. 21 B. 23 C. 25 D. 80

5.3.3 解析与答案

试题 1 分析

在 HDLC 通信方式中, 所有信息都是以帧的形式传送的。HDLC 定义了 3 种类型的帧, 每种类型都具有不同的控制字段格式。信息帧 (I) 携带的是向用户传输的数据。另外, 如果使用 ARQ 机制, 那么信息帧 (I) 中还捎带了流量控制和差错控制数据。管理帧 (S) 在未使用捎带技术时提供了 ARQ 机制。无编号帧 (U) 提供了增补的链路控制功能。控制字

段中的前一位或两位用作帧类型的标识。管理帧（S）的控制字段并不包含发送顺序号，因此备选项 B 是错误的。信息帧（I）发送顺序号占用 3 比特，取值范围是 0~7，因此备选项 C 也是错误的。

滑动窗口协议中，发送器每发出一个信息帧（I），窗口不向前滑动，只有等到确认后才把窗口向前滑动，因此备选项 D 是错误的；接收器如果收到一个正确的信息帧（I），并且发送顺序号落在接收窗口内，则发回确认帧，备选项 A 是正确的。

试题 1 答案

(1) A

试题 2 分析

X.25 描述了将一个分组终端连接到一个分组网络上所需要做的工作。通过虚电路它能负责维护一个通过单一物理连接的多用户会话，每个用户会话被分配一个逻辑信道。它提供了高优先级类型和正常优先级类型。

X.25 分为物理层、数据链路层、分组层 3 层，这 3 层对应于 OSI 模型的最底下 3 层。

物理层：规定用户主机或终端与分组交换网之间的物理接口，其标准为 X.21。

链路层：所用的标准是 LAP-B，是 HDLC 的一个子集。

分组层：提供外部虚电路服务。

三层之间的关系：用户数据被送到 X.25 第三层，在第三层加上含有控制信息的报头，从而组成了一个分组。控制信息用于协议的操作。整个 X.25 分组然后送到 LAP-B 实体，LAP-B 在此分组的前后各加上控制信息组成一个 LAP-B 帧，在帧中加入控制信息也是为了协议的操作。

X.25 的分组层提供虚电路服务，数据以分组形式通过外部虚电路传输。虚电路有两类型：呼叫虚电路，是通过呼叫建立和呼叫清除等过程动态地建立起来的虚电路；永久虚电路则是固定的虚电路。

由于 X.25 的分组层提供虚电路服务，是有连接的服务，因此备选项 A 是错误的。“网络丢失帧时，通过检查帧顺序号重传丢失帧”是有连接服务的特点，备选项 B 是正确的。

链路层所用的传输控制协议标准为 LAP-B，备选项 C 是错误的。X.25 网络采用虚电路来进行不同站点间的数据传输，备选项 D 是错误的。

试题 2 答案

(2) B

试题 3 分析

在数据报系统中，每个分组被视为独立的，它和以前发送的分组间没有什么关系。在前进的道路上，每个节点为分组选择下一个节点，因此分组虽然具有相同的目的地，但并不是按照相同的路由前进。备选项 A 是错误的。

在滑动窗口协议中，接收方收到一个正确的帧，并且发送顺序号落在接收窗口内，则发回确认帧，发送方根据确认帧的帧编号来向前滑动窗口，窗口内的帧可以连续发送，备选项 B 是正确的。

前向纠错技术（Forward Error Correction, FEC）长期以来一直与高级线路编码方案一起广泛应用在物理链路层。这些技术检查和纠正 WAN 链路上的比特错误，以确保上层协议收到无错误的数据报。前向纠错技术通过在发送每 N 个数据报后添加一个错误恢复包来纠正错误。这个 FEC 包内含可被用来构建由 N 个数据报组成的分组内的任意一个数据报的信息。如果这 N 个数据报中的一个恰巧在 WAN 传输过程中丢失，FEC 包用于在 WAN 链路的远端上重建丢失的数据报。这就消除了重新在 WAN 上传输丢失数据报的需要，从而大大减少应

用响应时间，提高 WAN 的效率。

TCP 协议中除了重传计时器管理外，也可以通过慢启动、拥塞时的动态调整窗口大小等窗口管理机制进行拥塞控制。备选项 D 是错误的。

试题 3 答案

(3) B

试题 4 分析

面向连接的方式功能强大，允许流量控制、差错控制以及顺序交付等。无连接的服务是不可靠的服务，无法许诺不会出现的交付和重复的差错，但这种协议代价很小，更适用于某些服务，比如内部的数据采集、向外的数据分发、请求-响应，以及实时应用等。因此在运输层既有面向连接的位置，也有无连接的用武之地。每一个分组独立地建立和释放逻辑连接，也适合传送大量的数据。

无连接的服务的通信线路不都是预设的。无连接的服务需要将目标地址信息加在每个发送的分组上，便于每个分组路由到达目的地。UDP 在电路交换或租用专线网络上也能运行。

试题 4 答案

(4) C

试题 5 分析

通过 IP 包传送的 ICMP 信息主要用于涉及网络操作或错误操作的不可达信息。ICMP 包发送是不可靠的，所以主机不能依靠接收 ICMP 包解决任何网络问题。

ICMP 的主要功能如下。

① 通告网络错误。比如，某台主机或整个网络由于某些故障不可达。如果有指向某个端口号的 TCP 或 UDP 包没有指明接收端，这也由 ICMP 报告。

② 通告网络拥塞。当路由器缓存太多包，由于传输速度无法达到它们的接收速度，将会生成“ICMP 源结束”信息。对于发送者，这些信息将会导致传输速度降低。当然，更多的 ICMP 源结束信息的生成也将引起更多的网络拥塞，所以使用起来较为保守。

③ 协助解决故障。ICMP 支持 Ech 功能，即在两个主机间一个往返路径上发送一个包。ping 是一种基于这种特性的通用网络管理工具，它将传输一系列的包，测量平均往返次数并计算丢失百分比。

④ 通告超时。如果一个 IP 包的 TTL 降低到零，路由器就会丢弃此包，这时会生成一个 ICMP 包通告这一事实。TraceRoute 是一个工具，它通过发送小 TTL 值的包及监视 ICMP 超时通告可以显示网络路由。

根据 MAC 地址查找对应的 IP 地址是 RARP 协议的功能。把公网的 IP 地址转换为私网的 IP 地址是 NAT 的功能。备选项 D 是拼凑的备选项。

试题 5 答案

(5) C

试题 6 分析

TCP 和 UDP 是 TCP/IP 协议中的两个传输层协议，它们使用 IP 路由功能把数据报发送到目的地，从而为应用程序及应用层协议（包括 HTTP、SMTP、SNMP、FTP 和 Telnet）提供网络服务。TCP 提供的是面向连接的、可靠的数据流传输，而 UDP 提供的是非面向连接的、不可靠的数据流传输。TCP 报头格式如图 5-10 所示。

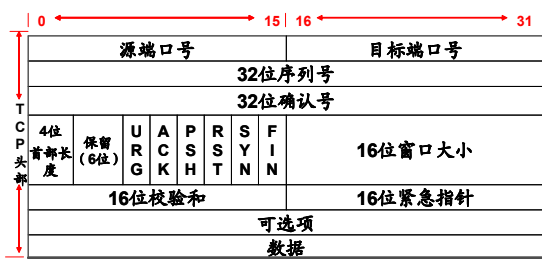


图 5-10 TCP 报头格式

TCP 首部的数据格式如上图所示。如果不计任选字段，它通常是 20 个字节。UDP 首部的各字段和 UDP 报头格式如图 5-11 所示。



图 5-11 UDP 报头格式

因此，顺序号包含在 TCP 头中而不包含在 UDP 头中。

试题 6 答案

(6) B

试题 7 分析

LAP-B 是 X.25 的数据链路层协议；X.21 是指 DTE-DCE 之间接口（物理上）的规定，这个在概念上类似于 RS-232，属于物理层的范畴；X.25 PLP 是 X.25 的网络层；MHS 是信息处理服务。

试题 7 答案

(7) C

试题 8 分析

在 TCP/IP 体系结构中，ARP 协议是知道对方的 IP 地址，解析出对方的 MAC 地址。

试题 8 答案

(8) A

试题 9 分析

在 TCP/IP 体系结构中，ARP 协议数据单元封装在以太网的数据帧中传送。

试题 9 答案

(9) A

试题 10 分析

端口号是传输层协议（TCP 或 UDP）向上边的应用层提供的服务访问点。0~1023 之间的端口号固定地分配给了常见的应用。用户自己开发的应用可以在 1025 ~65535 之间选择端口号。简单邮件传输协议默认的端口号是 25。

试题 10 答案

(10) C

5.4 考前冲刺

试题 1

关于 ARP 表, 以下描述中正确的是____(1)_____。

- (1) A. 提供常用目标地址的快捷方式来减少网络流量
- B. 用于建立 IP 地址到 MAC 地址的映射
- C. 用于在各个子网之间进行路由选择
- D. 用于进行应用层信息的转换

试题 2

在 FTP 协议中, 控制连接是由____(2)_____主动建立的。

- (2) A. 服务器端 B. 客户端 C. 操作系统 D. 服务提供商

试题 3

TCP 段头的最小长度是____(3)_____字节。

- (3) A. 16 B. 20 C. 24 D. 32

试题 4

以下关于 FTP 和 TFTP 描述中, 正确的是____(4)_____。

- (4) A. FTP 和 TFTP 都基于 TCP 协议
- B. FTP 和 TFTP 都基于 UDP 协议
- C. FTP 基于 TCP 协议, TFTP 基于 UDP 协议
- D. FTP 基于 UDP 协议, TFTP 基于 TCP 协议

试题 5

浏览器与 Web 服务器通过建立____(5)_____连接来传送网页。

- (5) A. UDP B. TCP C. IP D. RIP

试题 6

在 TCP 协议中, 采用____(6)_____来区分不同的应用进程。

- (6) A. 端口号 B. IP 地址 C. 协议类型 D. MAC 地址

试题 7

TCP 是互联网中的传输层协议, 使用____(7)_____次握手协议建立连接。

- (7) A. 1 B. 2 C. 3 D. 4

试题 8

ARP 协议的作用是由 IP 地址求 MAC 地址, ARP 请求是广播发送, ARP 响应是____(8)_____发送。

- (8) A. 单播 B. 组播 C. 广播 D. 点播

试题 9

ICMP 协议在网络中起到了差错控制和交通控制的作用。在 IP 数据报的传送过程中, 如果出现网络拥塞, 则路由器发出____(9)_____报文。

- (9) A. 路由重定向 B. 目标不可到达 C. 源抑制 D. 超时

试题 10

TCP 是互联网中的传输层协议, TCP 协议进行流量控制的方法是____(10)_____。

- (10) A. 使用停等 ARQ 协议 B. 使用后退 N 帧 ARQ 协议
- C. 使用固定大小的滑动窗口协议 D. 使用可变大小的滑动窗口协议

试题 11

TCP 实体发出连接请求 (SYN) 后, 等待对方的____(11)____响应。

- (11) A. SYN B. FIN, ACK C. SYN, ACK D. RST

试题 12

使用____(12)____协议远程配置交换机。

- (12) A. Telnet B. FTP C. HTTP D. PPP

试题 13

在 TCP/IP 网络中, 为各种公共服务保留的端口号范围是____(13)____。

- (13) A. 1~255 B. 256~1023 C. 1~1023 D. 1024~65535

试题 14

HDLCL 协议是一种____(14)____。

- (14) A. 面向比特的同步链路控制协议 B. 面向字节计数的同步链路控制协议
C. 面向字符的同步链路控制协议 D. 异步链路控制协议

试题 15

SSL 协议使用的默认端口是____(15)____。

- (15) A. 80 B. 445 C. 8080 D. 443

5.5 习题解析

试题 1 分析

ARP 协议的作用是由目标的 IP 地址发现对应的 MAC 地址。如果源站要和一个新的目标通信, 首先由源站发出 ARP 请求广播包, 其中包含目标的 IP 地址, 然后目标返回 ARP 应答包, 其中包含了自己的 MAC 地址。这时, 源站一方面把目标的 MAC 地址装入要发送的数据帧中, 一方面把得到的 MAC 地址添加到自己的 ARP 表中。当一个站与多个目标进行了通信后, 在其 ARP 表中就积累了多个表项, 每一项都是 IP 地址与 MAC 地址的映射关系。ARP 表通常用于由 IP 地址查找对应的 MAC 地址。

试题 1 答案

- (1) B

试题 2 分析

文件传输协议 FTP 利用 TCP 连接在客户机和服务器之间上传和下载文件。FTP 协议占用了两个 TCP 端口, FTP 服务器监听 21 号端口, 准备接受用户的连接请求。当用户访问 FTP 服务器时便主动与服务器的 21 号端口建立了控制连接。如果用户要求下载文件, 则必须等待服务器的 20 号端口主动发出建立数据连接的请求, 文件传输完成后数据连接随之释放。在客户端看来, 这种处理方式被叫做被动式 FTP, Windows 系统中默认的就是这种处理方式。由于有的防火墙阻止由外向内主动发起的连接请求, 所以 FTP 数据连接可能由于防火墙的过滤而无法建立。为此有人发明了一种主动式 FTP, 即数据连接也是由客户端主动请求建立的, 但是在服务器中接收数据连接的就不是 20 号端口了。

试题 2 答案

- (2) B

试题 3 分析

TCP 头部如图 5-12 所示:

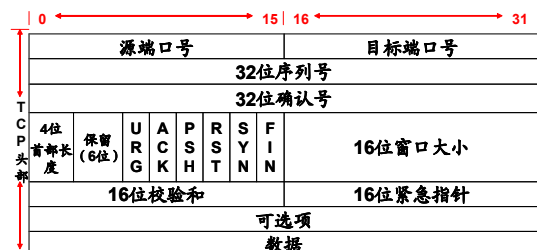


图 5-12 TCP 报头格式

除了“任选项+补丁”之外共有 5 行，20 个字节。

试题 3 答案

(3) B

试题 4 分析

本题考查 FTP 的基本知识。

FTP (File Transfer Protocol, 文件传输协议) 是 TCP/IP 的一种具体应用, 它工作在 OSI 模型的第 7 层, TCP 模型的第 4 层上, 即应用层, 使用 TCP 传输, FTP 连接是可靠的, 而且是面向连接, 为数据的传输提供了可靠的保证。

TFTP (Trivial File Transfer Protocol, 简单文件传送协议) 的功能与 FTP 类似, 但是为了保持简单和短小, TFTP 使用 UDP 协议。

试题 4 答案

(4) C

试题 5 分析

浏览器与 Web 服务器之间通过 HTTP 协议传送网页数据。支持 HTTP 协议的下层协议为 TCP 协议, 所以在开始传送网页之前浏览器与 Web 服务器必须先建立一条 TCP 连接。

试题 5 答案

(5) B

试题 6 分析

TCP 属于传输层协议, 它可以支持多种应用层协议。应用层协议访问 TCP 服务的访问点是端口号, 不同的端口号用于区分不同的应用进程。例如 HTTP 协议对应的端口号是 80, FTP 对应的端口号是 20 和 21。

试题 6 答案

(6) A

试题 7 分析

建立 TCP 连接需要收发双方进行三次握手。

试题 7 答案

(7) C

试题 8 分析

ARP 协议的作用是由 IP 地址求 MAC 地址。当源主机要发送一个数据帧时, 必须在本地的 ARP 表中查找目标主机的 MAC (硬件) 地址。如果 ARP 表查不到, 就广播一个 ARP 请求分组, 这种分组可到达同一子网中的所有主机, 它的含义是“如果你的 IP (协议) 地址

是这个，请回答你的 MAC 地址是什么”。收到该分组的主机一方面可以用分组中（发送节点的）的两个源地址更新自己的 ARP 表，另一方面用自己的 IP 地址与目标 IP 地址字段比较，若相符则发回一个 ARP 响应分组，向发送方报告自己的 MAC 地址，若不相符则不予回答。ARP 请求通过广播帧发送，ARP 响应通过单播帧发送给源站。

试题 8 答案

(8) A

试题 9 分析

ICMP (Internet Control Message Protocol) 属于网络层协议，用于传送有关通信问题的消息。ICMP 报文封装在 IP 数据报中传送，因而不保证可靠的提交。ICMP 报文有很多种类，用于表达不同的路由控制信息，其报文格式如图 5-13 所示。其中的类型字段表示 ICMP 报文的类型，代码字段可表示报文的少量参数，当参数较多时写入 32 位的参数字段，ICMP 报文携带的信息包含在可变长的信息字段中，校验和字段是关于整个 ICMP 报文的校验和。

类型	代码	校验和
参数		
信息 (可变长)		

图 5-13 ICMP 报文格式

下面简要解释 ICMP 各类报文的含义。

① 目标不可到达 (类型 3)：如果路由器判断出不能把 IP 数据报送达目标主机，则向源主机返回这种报文。另一种情况是目标主机找不到有关的用户协议或上层。

服务访问点也会返回这种报文。出现这种情况的原因可能是 IP 头中的字段不正确；或是数据报中说明的源路由无效；也可能是路由器必须把数据报分段，但 IP 头中的 D 标志已置位。

② 超时 (类型 11)：路由器发现 IP 数据报的生存期已超时，或者目标主机在一定时间内无法完成重装配，则向源端返回这种报文。

③ 源抑制 (类型 4)：这种报文提供了一种流量控制的初等方式。如果路由器或目标主机缓冲资源耗尽而必须丢弃数据报，则每丢弃一个数据报就向源主机发回一个源抑制报文，这时源主机必须减小发送速度。另外一种情况是系统的缓冲区已用完，并预感到将发生拥塞，则发出源抑制报文。但是与前一种情况不同，涉及的数据报尚能提交给目标主机。

④ 参数问题 (类型 12)：如果路由器或主机判断出 IP 头中的字段或语义出错，则返回这种报文，报文头中包含一个指向出错字段的指针。

⑤ 路由重定向 (类型 5)：路由器向直接相连的主机发出这种报文，告诉主机一个更短的路径。例如路由器 R1 收到本地网络上的主机发来的数据报，R1 检查它的路由表，发现要把数据报发往网络 X，必须先转发给路由器 R2，而 R2 又与源主机在同一网络中。于是 R1 向源主机发出路由重定向报文，把 R2 的地址告诉它。

⑥ 回声 (请求/响应，类型 8/0)：用于测试两个节点之间的通信线路是否畅通。收到回声请求的节点必须发出回声响应报文。该报文中的标识符和序列号用于匹配请求和响应报文。当连续发出回声请求时，序列号连续递增。常用的 PING 工具就是这样工作的。

⑦ 时间戳 (请求/响应，类型 13/14)：用于测试两个节点之间的通信延迟时间。请求方发出本地的发送时间，响应方返回自己的接收时间和发送时间。这种应答过程如果结合强制路由的数据报实现，则可以测量出指定线路上的通信延迟。

⑧ 地址掩码 (请求/响应，类型 17/18)：主机可以利用这种报文获得它所在的 LAN 的子网掩码。首先主机广播地址掩码请求报文，同一 LAN 上的路由器以地址掩码响应报文回答，告诉请求方需要的子网掩码。了解子网掩码可以判断出数据报的目标节点与源节点是否

在同一 LAN 中。

试题 9 答案

(9) C

试题 10 分析

TCP 使用可变大小的滑动窗口协议来进行流量控制。这种流控方案把肯定应答信号与控制窗口滑动的信号分开处理，在控制数据流动速率方面给接收方提供了更大的自由度。在基础网络可靠的情况下，这种控制策略能产生平滑的数据流动，在基础网络不可靠时，它还是一种差错控制手段。

试题 10 答案

(10) D

试题 11 分析

TCP 采用三次握手协议来建立和释放连接，如图 5-14 所示。

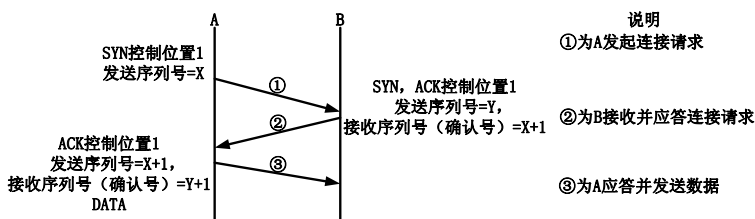


图 5-14 TCP 三次握手

可见，当 TCP 实体发出连接请求（SYN）后，等待对方的 SYN，ACK 响应。

试题 11 答案

(11) C

试题 12 分析

Telnet 协议的功能是远程登录。通过 Telnet 终端可以登录到远程交换机，进行配置和管理，前提是必须为交换机配置主机名或 IP 地址。Telnet 命令的一般格式为“telnet Hostname/IP 地址”。例如，在 Windows 的“运行”窗口中输入 Telnet 192.168.1.23 就可以登录到交换机进行配置了。

试题 12 答案

(12) A

试题 13 分析

端口号是传输层的服务访问点。在 TCP 和 UDP 报文中，端口号字段占 16 位，所以它的取值范围是 0~65535。常用的公共服务占用的端口号是 1~1023，端口 1024 保留，其他专用协议在 1025~65535 中选用端口号。

试题 13 答案

(13) C

试题 14 分析

数据链路控制协议分为面向字符的协议和面向比特的协议。面向字符的协议以字符作为传输的基本单位，并用 10 个专用字符控制传输过程。面向比特的协议以比特作为传输的基本单位，它的传输效率高，广泛地应用于公用数据网中。HDLC 是面向比特的数据链路控制

协议。

试题 14 答案

(14) A

试题 15 分析

本题属于记忆题。

80 端口是 Web 服务默认端口。8080 端口一般用于局域网内部提供 Web 服务。445 端口和 139 端口一样，用于局域网中共享文件夹或共享打印机。

试题 15 答案

(15) D

数据通信是通信技术和计算机技术相结合而产生的一种新的通信方式。要在两地间传输信息必须有传输信道，根据传输媒体的不同，有有线数据通信与无线数据通信之分。但它们都是通过传输信道将数据终端与计算机联结起来，从而使不同地点的数据终端实现软、硬件和信息资源的共享。

6.1 考点脉络

数据通信基础是网络工程师考试的非常重要的一个考点。

根据考试大纲，要求考生掌握以下几个方面的内容。

(1) 数据通信基础技术：包括信道特征、数字编码、调制与编码。

(2) 传输与交换技术：包括复用技术、差错控制技术。

从历年的考试试题来看，本章的考点在综合知识考试中的平均分数为 7 分，约为总分的 9.3%。考试试题主要集中在信道特征、数字编码、差错控制技术这 3 个知识点上。

6.2 数据通信基础技术

数据通信基础这个考点中，主要涉及信道特征、数字编码类型、PCM 编码这三方面的内容。

6.2.1 考点精讲

信道是以传输媒质为基础的信号通道。根据信道的特征及分析问题所需，可以把信道分为狭义信道和广义信道。狭义信道指各种传输媒质，包括传输电（或光）信号的物质。广义信道除了包括传输媒质外，还包括通信系统有关的变换装置。

不同的数字编码技术会有不同的数字编码类型，基本都有其特有的编码示意图。

PCM 编码是最常用的编码技术，又称为脉冲编码调制技术（PCM）。

1. 信道特征

对于本知识点的考查，关键在于了解信道的关键特性，香农公式、奈氏准则的理解与应用，主要是理解型与计算题目。

在数据通信技术中，人们一方面通过研究新的传输媒介来降低噪声的影响，另一方面则是研究更先进的数据调制技术，以更加有效地利用信道的带宽。因此，这也就引出了一个历年考试常常出现的考点：计算信道的数据速率。

信道的数据速率计算公式如图 6-1 所示。

从图 6-1 中，可以看出在计算信道的数据速率时有两种考虑，一是考虑噪声，二是考虑理想传输。

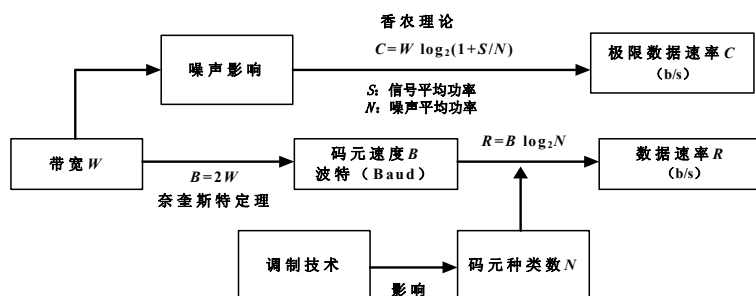


图 6-1 信道的数据速率计算公式

(1) 香农理论

在使用香农理论时，由于 S/N （信噪比）的比值通常太大，因此通常使用分贝数（dB）来表示： $\text{dB} = 10 \times \log_{10}(S/N)$ 。

例如， $S/N=1000$ 时，用分贝表示就是 30dB。如果带宽是 3kHz，则这时的极限数据速率就应该是： $C=3000 \times \log_2(1+1000) \approx 3000 \times 9.97 \approx 30\text{Kb/s}$ 。

对于有噪声的信道中，我们用误码率来表示传输二进制位时出现差错的概率（出错的位数/传送的总位数），通常的要求是小于 10^{-6} 。

(2) 奈奎斯特定理

奈奎斯特定理（也称为奈氏定理或尼奎斯特定理）的表达很简单，即 $R=2W\log_2 N$ 。

在计算时，最关键的在于理解码元和比特的转换关系。码元 N 是一个数据信号的基本单位，而比特是一个二进制位，即比特位，一位可以表示 2 个值。因此，如果码元可取 2 个离散值，则 N 值为 2，只需 1 比特表示。若可取 4 个离散值，则 N 值为 4，需要 2 比特来表示。

码元有多少个不同种类，取决于其使用的调制技术。如表 6-1 所示。关于调制技术的更多细节参见后面的知识点，在此只列出常见的调制技术所携带的码元数。

表 6-1 调制技术与码元数

调制技术	名称	码元种类	比特位
ASK	幅度键控	2	1
FSK	频移键控	2	1
PSK	相位键控（2 相调制）	2	1
DPSK	4 相键控调制	4	2
QPSK	正交相移键控	4	2

要注意的是，这两种算法得出的结论是不能够直接比较的，因为它们假设条件不同。在香农定理中，实际上也考虑了调制技术的影响，但由于高效的调制技术往往也会使出错的可能性更大，因此也会有一个极限，所以香农的计算方式忽略采用什么调制技术。另外，还值得一提的是，信道本身也会带来延迟，通常电缆中的传播速度是光速 $300\text{m}/\mu\text{s}$ 的 67%，即 $200\text{m}/\mu\text{s}$ 左右；而且根据距离不同也会增加延迟的值。

2. 数字编码与编码效率

对于本知识点来说，主要是要求能够根据编码示意图看出所采用的数据编码技术，了解各种技术的特点及应用领域。

二进制数字信息在传输过程中可采用不同的代码，这些代码的抗噪性和定时能力各不相同。最基本的数字编码有单极性码、极性码、双极性码、归零码、不归零码、双相码 6 种，常用于局域网的有曼彻斯特编码、差分曼彻斯特编码，常用于广域网的有 4B/5B 码、8B/10B 码。

(1) 基本编码

基本的编码方法有极性编码、归零性编码和双相码。

① 极性编码

极包括正极和负极。因此从这里就可以理解单极性码，就是只使用一个极性，再加零电平（正极表示 0，零电平表示 1）；极性码就是使用了两极（正极表示 0，负极表示 1）；双极性码则使用了正负两极和零电平（其中有一种典型的双极性码是信号交替反转编码 AMI，它用零电平表示 0，1 则使电平在正、负极间交替翻转）。码的极性变化如图 6-2 所示。

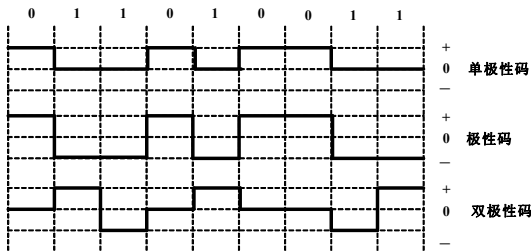


图 6-2 码的极性变化

在极性编码方案中，都是始终使用某一特定的电平来表示特定的数，因此当发送连续多个“1”或“0”时，将无法直接从信号判断出个数。要解决这个问题，就需要引入时钟信号。

② 归零性编码

归零指的是编码信号量是否回归到零电平。归零码就是指码元中间的信号回归到 0 电平。不归零码则不回归零（而是当 1 时电平翻转，0 时不翻转），也称之为差分机制。

③ 双相码

通过不同方向的电平翻转（低到高代表 0，高到低代表 1），这样不仅可以提高抗干扰性，还可以实现自同步，它也是曼码的基础。

归零码和双相码如图 6-3 所示。

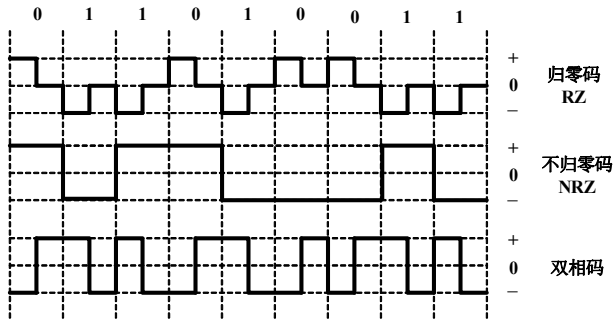


图 6-3 归零码和双相码

(2) 应用性编码

应用性编码主要有曼彻斯特编码、差分曼彻斯特编码、4B/5B 编码、8B/6T 编码和 8B/10B 编码等。

① 曼彻斯特编码和差分曼彻斯特编码

曼彻斯特编码和差分曼彻斯特编码如图 6-4 所示。

曼彻斯特编码是一种双相码，用低到高的电平转换表示 0，用高到低的电平转换表示 1（注意：某些教材中关于此相反的描述也是正确的），因此它也可以实现自同步，常用于以太网（802.3 10M 以太网）。

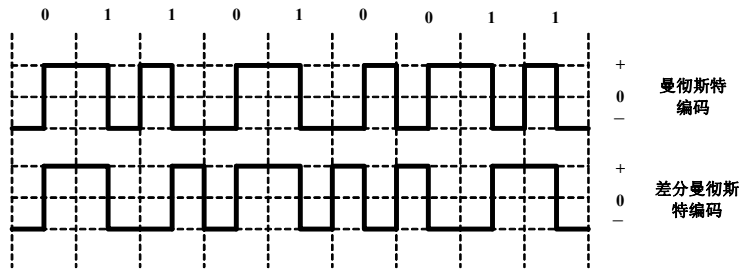


图 6-4 曼彻斯特编码和差分曼彻斯特编码

差分曼彻斯特编码是在曼彻斯特编码的基础上加上了翻转特性，遇 0 翻转，遇 1 不变，常用于令牌环网。要注意的一个知识点是：使用曼码和差分曼码时，每传输 1bit 的信息，就要求线路上有 2 次电平状态变化（2 Baud），因此要实现 100Mb/s 的传输速率，就需要有 200MHz 的带宽，即编码效率只有 50%。

② 4B/5B 编码、8B/6T 编码和 8B/10B 编码

正是因为曼码的编码效率不高，因此在带宽资源宝贵的广域网，以及速度要求更高的局域网中，就面临了困难。因此就出现了 $mBnB$ 编码，也就是将 m 位数据编码成 n 位符号（代码位）。

4B/5B 编码、8B/6T 编码和 8B/10B 编码的比较如表 6-2 所示。

表 6-2 应用编码标准

编 码 方 案	说 明	效 率	典 型 应 用
4B/5B	每次对 4 位数据进行编码，将其转为 5 位符号	1.25 波特/位 即 80%	100Base-FX、100Base-TX、FDDI
8B/10B	每次对 8 位数据进行编码，将其转为 10 位符号	1.25 波特/位 即 80%	千兆以太网
8B/6T	8bit 映射为 6 个三进制位	0.75 波特/位	100Base-T4

4. 调制技术

对于本知识点来说，主要是了解各种调制技术的特点，知道编码技术的实际用途。

最基本的调制技术包括幅度键控（ASK）、频移键控（FSK）和相移键控（PSK），它们之间的特性如表 6-3 所示。

表 6-3 调制技术及其特性

调 制 技 术	说 明	特 点
ASK	用恒定的载波振幅值表示一个数（通常是 1），无载波表示另一个数	实现简单，但抗干扰性差、效率低（典型数据率仅为 1200b/s）
FSK	由载波频率（ f_c ）附近的两个频率（ f_1 、 f_2 ）表示两个不同值， f_c 恰好为中值	抗干扰性较 ASK 更强，但占用带宽较大，典型速度也是 1200b/s
PSK	用载波的相位偏移来表示数据值	抗干扰性最好，而且相位的变化可以作为定时信息来同步时钟

最常用的是脉冲编码调制技术（PCM），简称脉码调制。关于 PCM 原理中有以下几个关键知识点。

（1）PCM 要经过取样、量化、编码三个步骤。

（2）根据奈奎斯特取样定理，取样速率应大于模拟信号的最高频率的 2 倍。我们都知道 44kHz 的音乐让人感觉到最保真，这是因为人耳可识别的最高频率约为 22kHz，因此当采样率达到 44kHz 时就可以得到最满意的效果。

（3）量化是将样本的连续值转成离散值，采用的方法类似于求圆周长时，用内切正多边形的方法。而平时，我们说 8 位、16 位的声音，指的就是 2^8 、 2^{16} 位量化。

（4）编码就是将量化后的样本值变成相应的二进制代码。

6.2.2 一点一练

试题 1

图 6-5 中画出曼彻斯特编码和差分曼彻斯特编码的波形图，实际传送的比特串为 （1）。

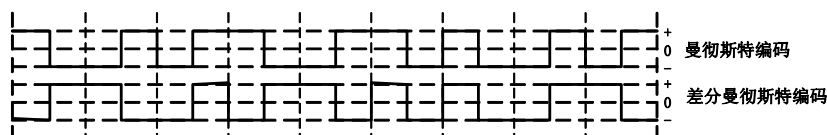


图 6-5 曼码和差分曼码的波形图

- （1） A. 0 1 1 0 1 0 0 1 1 B. 0 1 1 1 1 0 0 1 0
C. 1 0 0 1 0 1 1 0 0 D. 1 0 0 0 0 1 1 0 1

试题 2

双极型 AMI 编码经过一个噪声信道，接收的波形如图 6-6 所示，那么出错的是第 （2） 位。

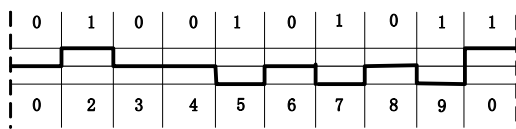


图 6-6 波形效果图

- （2） A. 3 B. 5 C. 7 D. 9

试题 3

图 6-7 中 12 位曼彻斯特编码的信号波形表示的数据是 （3）。

- （3） A. 100001110011 B. 111100110011 C. 011101110011 D. 011101110000

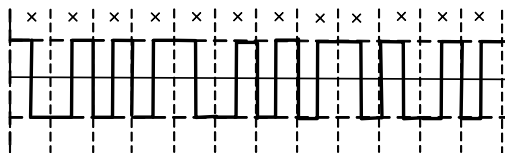


图 6-7 波形效果图

试题 4

设信道带宽为 4kHz，信噪比为 30dB，按照香农定理，信道的最大数据速率约等于 （4）。

- (4) A. 10Kb/s B. 20Kb/s C. 30Kb/s D. 40Kb/s

试题 5

下面关于 DPSK 调制技术的描述, 正确的是____(5)____。

- (5) A. 不同的码元幅度不同
B. 不同的码元前沿有不同的相位改变
C. 由 4 种相位不同的码元组成
D. 由不同的频率组成不同的码元

试题 6

图 6-8 所示的 4 种编码方式中属于差分曼彻斯特编码的是____(6)____。

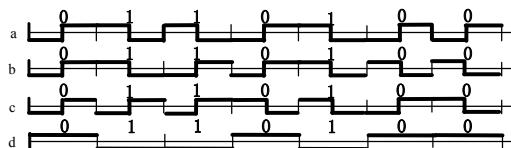


图 6-8 4 种编码图

- (6) A. a B. b C. c D. d

试题 7

下图的两种编码方案如图 6-9 所示, 二者分别是____(7)____。

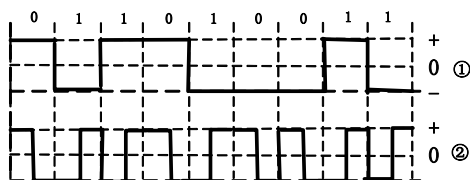


图 6-9 两种波形效果图

- (7) A. ① 差分曼彻斯特编码, ② 双相码
B. ① NRZ 编码, ② 差分曼彻斯特编码
C. ① NRZ-I 编码, ② 曼彻斯特编码
D. ① 极性码, ② 双极性码

试题 8

在异步通信中, 每个字符包含 1 位起始位、7 位数据位、1 位奇偶位和 2 位终止位, 若每秒钟传送 100 个字符, 采用 4 相相位调制, 则码元速率为____(8)____。

- (8) A. 50 波特 B. 500 波特
C. 550 波特 D. 1100 波特

试题 9

设信道带宽为 3400Hz, 调制为 4 种不同的码元, 根据尼奎斯特定理, 理想信道的数据速率为____(9)____。

- (9) A. 3.4Kb/s B. 6.8Kb/s C. 13.6Kb/s D. 34Kb/s

试题 10

图 6-10 所示是一种____(10)____调制方式。

- (10) A. ASK B. FSK C. PSK D. DPSK

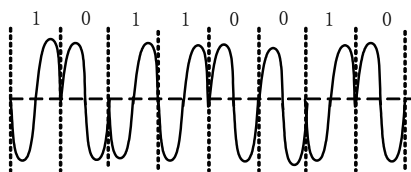


图 6-10 某种调制方式波形效果图

6.2.3 解析与答案

试题 1 分析

本题考查曼彻斯特编码和差分曼彻斯特编码的特性。

曼彻斯特编码特点：在每个比特间隙中间的电平跳变来同时代表比特位和同步信息。负电平到正电平的跳变代表比特 1，而正电平到负电平的跳变则代表比特 0。

差分曼彻斯特编码的特点：每比特的开始位置没有电平跳变表示比特 1，有电平跳变表示比特 0。

试题 1 答案

(1) A

试题 2 分析

信号交替反转编码 (Alternate Mark Inversion, AMI) 是一种典型的双极性码。在 AMI 信号中，数据流遇到“1”时，使电平在正和负之间交替翻转，而遇到“0”时，则保持零电平。这种双极性码是三进制信号的编码方法，它与二进制相比，抗噪性能更好。AMI 有其内在的检错能力，在正负脉冲交替出现的规律被打乱时容易识别出来，这种情况叫 AMI 违例。正确的编码如图 6-11 所示。

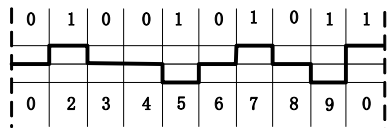


图 6-11 AMI 编码

这种编码方案的缺点是传送长串 0 时，会失去比特同步信息。

试题 2 答案

(2) C

试题 3 分析

曼彻斯特编码属于双相码，每一位都有电平跳变，包含一个低电平码元和一个高电平码元，电平跳变用于位同步，因而不需要附加外同步信息。曼彻斯特编码用高电平到低电平的跳变表示数据“0”，用低电平到高电平的跳变表示数据“1”。也有的系统中采用相反的方法，即用低电平到高电平的跳变表示数据“0”，用高电平到低电平的跳变表示数据“1”，这两种方法是等价的。图中表示的数据是 011101110011。

试题 3 答案

(3) C

试题 4 分析

在有噪声信道中，香农 (Shannon) 定理计算出的信道容量为：

$$C=W\log_2(1+S/N)$$

其中, W 为信道带宽, S 为信号的平均功率, N 为噪声平均功率, S/N 叫做信噪比。由于在实际使用中 S 与 N 的比值太大, 故常取其分贝数 (dB), 分贝与信噪比的关系为: $\text{dB}=10\times\log_{10}S/N$ 。

例如当 $S/N=1000$ 时, 信噪比为 30dB。这个公式与信号取的离散值个数无关, 也就是说无论用什么方式调制, 只要给定了信噪比, 则单位时间内最大的信息传输量就确定了。根据题意, 信道带宽为 4000Hz, 信噪比为 30dB, 则最大数据速率为:

$$C=4000\times\log_2(1+1000)\approx 4000\times 9.97\approx 40\text{Kb/s}$$

试题 4 答案

(4) D

试题 5 分析

DPSK 是一种差分相位调制技术 (Differential Phase Shift Keying), 即用不同的相位变化表示数据, 例如对于位 0, 前沿有相位变化, 对于位 1, 前沿没有相位变化, 如图 6-12 所示。

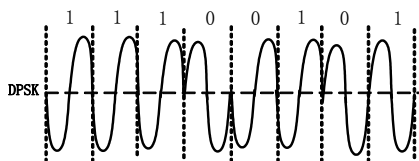


图 6-12 差分相位调制

试题 5 答案

(5) B

试题 6 分析

差分曼彻斯特编码是一种双相码。与曼彻斯特编码相同的地方是, 每一位都由一正一负两个码元组成, 但它又是一种差分码, 0 位的前沿有相位变化, 1 位的前沿没有相位变化, 所以选项 b 图形是差分曼彻斯特编码。

试题 6 答案

(6) B

试题 7 分析

在图①中, 每个“0”比特的前沿没有电平跳变, 每个“1”比特的前沿有电平跳变, 这是典型的 NRZ-I 编码的波形。NRZ-I 编码的数据速率与码元速率一致, 其缺点是当遇到长串的“0”时会失去同步, 所以有时要做出某种变通, 例如采用 4B/5B 编码。

曼彻斯特编码和差分曼彻斯特编码都属于双相码。双相码要求每一比特中间都有一个电平跳变, 它起到自定时的作用。在图②中, 我们用高电平到低电平的转换边表示“0”, 用低电平到高电平的转换边表示“1”, 这是曼彻斯特编码的一种实现方案。反之, 如果用高电平到低电平的转换边表示“1”, 而用低电平到高电平的转换边表示“0”, 也可以认为是曼彻斯特编码, 只要能区分两种不同的状态就可以了。比特中间的电平转换边既表示了数据代码, 也作为定时信号使用。曼彻斯特编码用在低速以太网中。

差分曼彻斯特编码与曼彻斯特编码不同, 码元中间的电平转换边只作为定时信号, 而不表示数据。数据的表示在于每一位开始处是否有电平转换: 有电平转换表示“0”, 无电平转换表示“1”, 差分曼彻斯特编码用在令牌环网中。

在曼彻斯特编码和差分曼彻斯特编码的图形中可以看出, 这两种双相码的每一个码元都要调制为两个不同的电平, 因而调制速率是码元速率的二倍。这对信道的带宽提出了更高的要求, 所以在数据速率很高时实现起来更昂贵, 但由于其良好的抗噪声特性和比特同步能力,

所以在局域网中仍被广泛使用。

试题 7 答案

(7) C

试题 8 分析

根据题中给出的条件, 每个字符要占用 $1+7+1+2=11$ (位)。每秒钟传送 100 个字符, 则数据速率为 $11 \times 100 = 1100 \text{ b/s}$ 。在采用 4 相相位调制(4PSK)的情况下, 数据速率为码元速率的 2 倍, 所以码元速率为 550 波特。

试题 8 答案

(8) C

试题 9 分析

按照 Nyquist 定理, $B=2W$ (Baud)。

码元速率为信道带宽的两倍。同时数据速率还取决于码元的离散状态数, 码元携带的信息量 n (比特数) 与码元的离散状态数 N 有如下关系: $n = \log_2 N$ 。

所以, 综合考虑了信道带宽和码元的离散状态数后得到的公式为:

$$R = B \log_2 N = 2W \log_2 N \text{ (b/s)}$$

其中, R 表示数据速率, 单位是 b/s。据此, 数据速率可计算如下:

$$R = B \log_2 N = 2W \log_2 N = 2 \times 3400 \times \log_2 4 = 6800 \times 2 = 13.6 \text{ Kb/s}$$

试题 9 答案

(9) C

试题 10 分析

数字数据在传输中可以用模拟信号来表示。用数字数据调制模拟载波信号的三个参数——幅度、频率和相位, 分别称为幅度键控、频移键控和相移键控。

按照幅度键控(ASK)调制方式, 载波的幅度受到数字数据的调制而取不同的值, 例如对应二进制 0, 载波振幅为 0; 对应二进制 1, 载波振幅取 1。调幅技术实现起来简单, 但抗干扰性能差。频移键控(FSK)是按照数字数据的值调制载波的频率。例如对应二进制 0 的载波频率为 f_1 , 而对应二进制 1 的载波频率为 f_2 。这种调制技术抗干扰性能好, 但占用带宽较大。在有些低速的调制解调器中, 用这种调制技术把数字数据变成模拟音频信号传送。相移键控(PSK)是用数字数据的值调制载波相位, 例如用 180 相移表示 1, 用 0 相移表示 0。这种调制方式抗干扰性能最好, 而且相位的变化也可以作为定时信息来同步发送机和接收机的时钟。码元只取两个相位值称为 2 相调制, 码元可取 4 个相位值称为 4 相调制。4 相调制时, 一个码元代表两位二进制数, 采用 4 相或更多相的调制能提供较高的数据速率, 但实现技术更复杂。三种数字调制方式表示如图 6-13 所示。

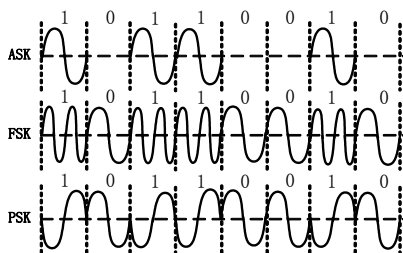


图 6-13 三种模拟调制方式示意图

6.3 传输交换与差错控制技术

在传输交换技术与差错控制技术这个考点中，主要涉及多路复用技术、海明校验、CRC 校验这三方面的内容。

6.3.1 考点精讲

数据通信系统或计算机网络系统中，传输媒体的带宽或容量往往会超过传输单一信号的需求，为了有效地利用通信线路，希望一个信道同时传输多路信号，这就是所谓的多路复用技术 (Multiplexing)。采用多路复用技术能把多个信号组合起来在一条物理信道上进行传输，在远距离传输时可大大节省电缆的安装和维护费用。

海明校验和 CRC 校验是差错控制技术中非常重要的两个检错技术。

1. 数据通信与交换方式

对于本知识点来说，主要是能够从原理性上了解各种通信方式和交换方式，特别是要扎实地掌握各种交换方式的过程、开销、特点及主要代表。

(1) 数据通信方式

按照数据传输方向，可以分为三种：单工通信，即信息只能在一个方向传送，如无线电广播、有线电视等；半双工通信，即双方可交替发送和接收信息，但不能够同时接收和发送，如无线电台、对讲机，由于相对全双工而言，设备价格更低，因此通常在要求不高时使用；全双工通信，即可以同时双向信息传送，如现代电话通信。

按同步方式可以分为两种：一是异步传输，即将各个字符分开传输，字符间插入诸如“起始位”、“终止位”的同步信息，而且通常还需要加入“校验信息”，适合长距离传输；二是同步传输，即顺序地连续传输，通常是在传输前进行同步，然后在传输时双方以同一频率工作，这种通信方式通常用于短距离高速数据传输，如磁盘访问。

(2) 交换方式

通信网络中通常有许多中间节点，因此信息在传输时需要经过许多中间节点，这些交换节点转发信息的方式就是交换方式。表 6-4 列出了几种常见的交换方式的对比。

表 6-4 常见的交换方式的对比

交 换 方 式		主 要 特 点	传 输 时 间
电路交换		首先创建一条临时专用通路(通常包括一系列链路)，使用完后拆除链接，没有传输延迟，适合大量数据传输和实时通信，少量信息传输时效率不高	链路建立时间+链路延迟时间+数据传输时间
报文交换		不在通信节点间建立通路，将信息组合为报文，采用虚储-转发的机制，线路利用率高，但传输延迟较大	(链路延时时间+中间节点延迟时间+报文传送时间)×报文数
分组交换 (数据包定长的报文交换，交换节点的缓冲区可减少，传播时延也更小)	数据报	类似于报文交换，发送端要组合成分组，接收端要拆分，通常使用 PAD (分组装/拆设备)	(链路延时时间+中间节点延迟时间+分组传送时间)×分组数
	虚电路	类似于电路交换，要建立一个逻辑链路，但逻辑链路是共享的。可靠性高，但效率要低于数据报	链路建立时间+(链路延时时间+中间节点延迟时间+分组传送时间)×分组数
	信元交换	采用 53B 的永远固定的分组大小，通常是采用面向连接的虚电路方式，ATM 使用该方式	链路建立时间+(链路延时时间+中间节点延迟时间+信元传送时间)×信元数

2. 复用技术

对于本知识点来说，主要了解多路复用技术的类型、技术要点和应用点，包括要对复用的产物 T1、E1 有一定了解。

(1) 多路复用技术

常见的多路复用技术包括频分多路复用（FDM）、时分多路复用（TDM）和波分多路复用（WDM），其中时分多路复用又包括同步时分复用和统计时分复用。表 6-5 中列出了它们的关键知识点。

表 6-5 复用技术及其特性

复 用 技 术		特 点 与 描 述	典 型 应 用
FDM		在一条传输介质上使用多个不同频率的模拟载波信号进行传输，每个载波信号形成一个不重叠、相互隔离（不连续）的频带。接收端通过带通滤波器来分离信号	无线电广播系统 有线电视系统（CATV） 宽带局域网 模拟载波系统
TDM	同步 TDM	每个子通道按照时间片轮流占用带宽，但每个传输时间划分为固定大小的周期，即使子通道不使用也不能够给其他子通道使用	T1/E1 等数字载波系统 ISDN 用户网络接口 SONET/SDH（同步光纤网络）
	统计 TDM	是对同步时分复用的改进，固定大小的周期可以根据子通道的需求动态地分配	ATM
WDM		与 FDM 相同，只不过不同子信道使用的是不同波长的光波来承载，而非频率，常用到 ILD	用于光纤通信

(2) 常见复用标准

在电话的语音通信中，通常是对 4kHz 的话音通道按 8kHz 的速率采样，用 128 级（ 2^7 ，因此需要 7bit）量化，因此每个话音信道的比特率是 56Kb/s。而由于在传输时，需要在每个 7bit 组后加上 1bit 的信令位，因此构成了 64Kb/s 的数字信道。

常见的复用标准如表 6-6 所示。

表 6-6 常见的复用标准

名 称	原理与组成	应 用 地 区
T1 载波（一次群，DS1）	采用同步时分复用技术将 24 个话音通路（每个话音信道称为 DS0）复合在一条 1.544Mb/s 的高带信道上	美国和日本
E1 载波	采用同步时分复用技术将 30 个话音信道（64Kb/s）和 2 个控制信道（16Kb/s）复合在一条 2.048Mb/s 的高速信道上	欧洲发起，除美、日外多用
T2（DS2）	由 4 个 T1 时分复用而成，达到 6.312Mb/s	美国和日本
T3（DS3B）	由 7 个 T2 时分复用而成，达到 44.736Mb/s	美国和日本
T4（DS4B）	由 6 个 T3 时分复用而成，达到 274.176Mb/s	美国和日本

3. 流控技术

本知识点最重要的是理解流量控制技术的意义，知道停等协议常用于单工通信，滑动窗口协议常用于双工通信，掌握两种基本的流控技术、三种自动重发技术的概念，并知道它们结合使用所产生的 5 种协议，能够分别计算出各种协议的最佳链路利用率。

表 6-7 总结了 5 种流量控制技术的特点和计算链路利用率方法等知识点。

表 6-7 流量控制与链路利用率

协议名称	特点	链路利用率
停等协议 (单工通信)	发送站每传送一帧,就停止发送,等收到应答信号后再发送下一帧。在局域中效率较高,对广域网而言效率太低	$E=1/(2a+1)$ a : 帧计数长度
滑动窗口协议 (双工通信)	允许连续发送多个帧而无须等待应答,所允许的这个帧数是固定值,也称为窗口。当成功收到一个确认包后,窗口就向前滑动 1 位	$E=W/(2a+1)$
停等 ARQ 协议 (有噪声环境的单工通信)	它是停等协议和自动请求重发技术的结合,发送站每传送一帧,就停止发送,等收到肯定应答信号(ACK)后再发送下一帧,如果收到否定应答(NAK)后重发该帧,在一定时间间隔内未收到 ACK,也重发	$E=(1-P)/(2a+1)$ P : 帧出错概率
选择重发 ARQ (有噪声环境的双工通信)	它是滑动窗口协议与自动请求重发技术的结合,当收到否定应答(NAK)时,只重发出错的帧。为了避免异常,其最大值就小于帧编号总数的一半,即 $W_{发}=W_{收}\leq 2^{K-1}$	若窗口值 $>2a+1$, 则 $E=1-P$; 窗口值 $\leq 2a+1$, 则 $E=W(1-P)/(2a+1)$ W : 窗口值
后退 N 帧 ARQ (有噪声环境的双工通信)	也是滑动窗口协议与自动请求重发技术的结合,只是当收到否定应答(NAK)时,将从出错处重发已发出过的 N 个帧。为了避免异常,必须限制发送窗口的大小 $W\leq 2^{K-1}$ (K 为帧编号的位数)	若窗口值 $>2a+1$, 则 $E=(1-P)/(1-P+NP)$; 若窗口值 $\leq 2a+1$, 则 $E=W(1-P)/(2a+1)(1-P+NP)$

注: 其中帧计算长度 a 的计算方法有: (传播延迟/发送一帧的时间)、(数据速率 \times 线路长度/传播速度/帧长)、(数据速率 \times 传播延迟/帧长)三种,最后一种最常用。

在后退 N 帧 ARQ 协议中的链路利用率计算公式中的 N 是重发的帧数,当窗口值 $>2a+1$ 时, N 近似于 $2a+1$; 当窗口值 $\leq 2a+1$ 时, $N=W$ 。

此外,还有一个需要注意的知识点是: 在全双工通信中应答信号可以由反方向传送的数据帧“捎带”送回,也就是不需要单独的帧。

4. 差错控制技术

对于本知识点来说,主要需要掌握海明码与 CRC 两种检错/纠错机制,能够理解码距,计算校验码,根据校验码判断是否出错,利用海明码找出错误位,了解主要的 CRC 应用等。

(1) 海明校验

可以在数据代码上添加若干冗余位组成码字。而将一个码字变成另一个码字时必须改变的最小位数就是码字之间海明距离,简称码距。码距是不同码字的海明距离的最小值。

① 可查出多少位错误: 可以发现“ \leq 码距-1”位的错误。

② 可以纠正多少位错误: 可以纠正“ $<$ 码距/2”位的错误,因此如果要能够纠正 n 位错误,则所需最小的码距应该是 $2n+1$ 。

要计算海明校验码,首先要知道海明校验码是放置在 2 的幂次位上的,即 1, 2, 4, 8, 16, 32, ..., 而对于信息位为 m 的原始数据,需加入 k 位的校验码,它满足 $m+k+1\leq 2^k$ 。而有一种简单的方法,则是从第 1 位开始写,遇到校验位留下空格。例如,原始信息为 101101100,并采用偶校验,则如图 6-14 所示。

然后根据以下公式填充校验位“1, 2, 4, 8”:

$$\text{Bit } 1=B_3 \oplus B_5 \oplus B_7 \oplus B_9 \oplus B_{11} \oplus B_{13}=1 \oplus 0 \oplus 1 \oplus 0 \oplus 1 \oplus 0=1$$

$$\text{Bit } 2=B_3 \oplus B_6 \oplus B_7 \oplus B_{10} \oplus B_{11}=1 \oplus 1 \oplus 1 \oplus 1 \oplus 1=1$$

Bit 4=B5 ⊕ B6 ⊕ B7 ⊕ B12 ⊕ B13 = 0 ⊕ 1 ⊕ 1 ⊕ 0 ⊕ 0 =0

Bit 8=B9 ⊕ B10 ⊕ B11 ⊕ B12 ⊕ B13 = 0 ⊕ 1 ⊕ 1 ⊕ 0 ⊕ 0=0

注：⊕指的是半加-进位加法、异或；Bn 代表位数。

		1		0	1	1		0	1	1	0	0
1	2	3	4	5	6	7	8	9	10	11	12	13

图 6-14 采用偶校验

最后将结果填入，得到如图 6-15 所示的结果。

1	1	1	0	0	1	1	0	0	1	1	0	0
1	2	3	4	5	6	7	8	9	10	11	12	13

图 6-15 添加校验码后的结果

而如果给出一个加入了校验码的信息，并说明有一位错误，要找出，则可以采用基本相同的方法，假如给出的是如图 6-16 所示的情况。

1	1	1	0	0	1	1	0	0	1	0	0	0
1	2	3	4	5	6	7	8	9	10	11	12	13

图 6-16 用于纠错的例子

可根据以下公式计算：

Bit 1=B1 ⊕ B3 ⊕ B5 ⊕ B7 ⊕ B9 ⊕ B11 ⊕ B13 = 1 ⊕ 1 ⊕ 0 ⊕ 1 ⊕ 0 ⊕ 0 ⊕ 0 =1

Bit 2=B2 ⊕ B3 ⊕ B6 ⊕ B7 ⊕ B10 ⊕ B11 = 1 ⊕ 1 ⊕ 1 ⊕ 1 ⊕ 1 ⊕ 0 =1

Bit 4=B4 ⊕ B5 ⊕ B6 ⊕ B7 ⊕ B12 ⊕ B13 = 0 ⊕ 0 ⊕ 1 ⊕ 1 ⊕ 0 ⊕ 0 =0

Bit 8=B8 ⊕ B9 ⊕ B10 ⊕ B11 ⊕ B12 ⊕ B13 = 0 ⊕ 0 ⊕ 1 ⊕ 0 ⊕ 0 ⊕ 0 =1

然后从高位往下写，得到 1011，即十进制的 11，因此出错的位数为第 11 位。这个过程如表 6-8 所示。

表 6-8 纠错的过程

	1	2	3	4	5	6	7	8	9	10	11	12	13
B8	0	0	0	0	0	0	0	1	1	1	1	1	1
B4	0	0	0	1	1	1	1	0	0	0	0	1	1
B2	0	1	1	0	0	1	1	0	0	1	1	0	0
B1	1	0	1	0	1	0	1	0	1	0	1	0	1

(2) CRC 校验

CRC 由于其实现的原理十分易于用硬件实现，因此广泛地应用于计算机网络上的差错控制。而 CRC 的考查点主要有 3 个：常见的 CRC 应用标准、计算 CRC 校验码、验算一个加了 CRC 校验的码是否有错误。

(1) 常见的 CRC 校验位

常见的 CRC 标准及应用可以归纳为表 6-9 所示。

表 6-9 CRC 标准及应用

网 络 协 议	CRC 位	应 用 点
HDLC	CRC16/CRC32	除帧标志位外的全帧

续表

网 络 协 议	CRC 位	应 用 点
FR (帧中继)	CRC16	除帧标志位外的全帧
ATM	CRC8	帧头校验
以太网 (802.3)	CRC32	帧头 (不含前导和帧起始符)
令牌总线 (802.4)	CRC32	帧头 (不含前导和帧起始符)
令牌环 (802.5)	CRC32	帧头 (从帧控制字段到 LLC)
FDDI	CRC32	帧头 (从帧控制字段到 INFO)

(2) 计算 CRC 校验码

要计算 CRC 校验码, 需根据 CRC 生成多项式进行。例如: 原始报文为 11001010101, 其生成多项式为 x^4+x^3+x+1 。在计算时, 在原始报文的后面添加若干个 0 (0 的个数等于校验码的位数, 而生成多项式的最高幂次就是校验位的位数, 即使用该生成多项式产生的校验码为 4 位) 作为被除数, 除以生成多项式所对应的二进制数 (根据其幂次的值决定, 得到 11011, 因为生成多项式中除了没有 x^2 之外, 其他位都有)。然后使用模 2 除, 得到的商就是校验码, 如图 6-17 所示。

$$\begin{array}{r}
 11011 \overline{) 110010101010000} \\
 \underline{11011} \\
 10010 \\
 \underline{11011} \\
 10011 \\
 \underline{11011} \\
 10000 \\
 \underline{11011} \\
 10111 \\
 \underline{11011} \\
 11000 \\
 \underline{11011} \\
 11000 \\
 \underline{11011} \\
 00011 \rightarrow 0011
 \end{array}$$

图 6-17 计算 CRC 校验码

然后将 0011 添加到原始报文的后面, 就是结果 110010101010011。

(3) 检查信息码是否有 CRC 错误

要想检查信息码是否出现了 CRC 错误的计算很简单, 只需用待检查的信息码做被除数, 除以生成多项式, 如果能够整除就说明没有错误, 否则就是出错了。另外要注意的是, 当 CRC 检查出现错误时, 它是不会进行纠错的, 通常是让信息的发送方重发一遍。

6.3.2 一点一练

试题 1

使用海明码进行前向纠错, 如果冗余位为 4 位, 那么信息位最多可以用到 (1) 位。

- (1) A. 6 B. 8 C. 11 D. 16

试题 2

使用海明码进行前向纠错, 假定码字为 a6a5a4a3a2a1a0, 并且有下面的监督关系式:

$$S_2 = a_2 + a_4 + a_5 + a_6$$

$$S_1 = a_1 + a_3 + a_5 + a_6$$

$$S_0 = a_0 + a_3 + a_4 + a_6$$

若 $S_2 S_1 S_0 = 110$, 则表示出错位是 (2) 。

- (2) A. a3 B. a4 C. a5 D. a6

试题 3

若采用后退 N 帧 ARQ 协议进行流量控制, 帧编号为 7 位, 则发送窗口的最大长度为 (3)。

- (3) A. 7 B. 8 C. 127 D. 128

试题 4

若信息码字为 11100011, 生成多项式 $G(x)=x^5+x^4+x+1$, 则计算出的 CRC 校验码为 (4)。

- (4) A. 01101 B. 11010 C. 001101 D. 0011010

试题 5

海明码 (Hamming Code) 是一种 (5)。

- (5) A. 纠错码 B. 检错码 C. 语音编码 D. 压缩编码

6.3.3 解析与答案

试题 1 分析

本题考查海明编码知识。

海明码属于线性分组编码方式, 大多数分组码属于线性编码, 其基本原理是, 信息码元与校验码元通过线性方程式联系起来。

海明码的编码规则是: 如果有 n 个数据位和 k 个冗余校验位, 那么必须满足 $2^k-1 \geq n+k$, 此处 $k=4$, 因此有 $n \leq 2^{k-1}-1-k=16-1-4=11$, n 最大为 11。

试题 1 答案

- (1) C

试题 2 分析

由于 S2 S1 S0=110, S0 没有错, 在 S0 的监督式中涉及的 a0,a3,a4,a6 都没有错误。而 S2 和 S1 都为 1, 则说明 S2 和 S1 出错, 得出最终出错的位是 a5。

试题 2 答案

- (2) C

试题 3 分析

采用后退 N 帧 ARQ 协议, 在全双工通信中应答信号可以由反方向传送的数据帧“捎带”送回, 这种机制进一步减少了通信开销, 然而也带来了一些问题。在捎带应答方案中, 反向数据帧中的应答字段总是捎带一个应答信号, 这样就可能出现对同一个帧的重复应答。假定帧编号字段为 3 位长, 发送窗口大小为 8。当发送器收到第一个 ACK1 后把窗口推进到后沿为 1、前沿为 0 的位置, 即发送窗口现在包含的帧编号为 1、2、3、4、5、6、7、0, 如下所示。

1 2 3 4 5 6 7 0

如果这时又收到一个捎带回的 ACK1, 发送器如何动作呢? 后一个 ACK1 可能表示窗口中的所有帧都未曾接收, 也可能意味着窗口中的帧都已正确接收。这样协议就出现了二义性。然而, 如果规定窗口的大小为 7, 则就可以避免这种二义性。所以, 在后退 N 帧协议中必须限制发送窗口大小 $W_{\text{发}} \leq 2^{K-1}$ 。根据类似的推理, 对于选择重发 ARQ 协议, 发送窗口和接收窗口的最大值应为帧编号数的一半, 即 $W_{\text{发}}=W_{\text{收}} \leq 2^{K-1}$ 。

试题 3 答案

(3) C

试题 4 分析

由生成多项式 $G(x)=x^5+x^4+x+1$ 可以得到除数 110011, 由多项表达式中 x 的最高幂次为 5 可知, 被除数应该是信息码字后面加 5 个 0。然后用被除数与除数做模二除法得到的结果就是校验码, 其计算结果是 11010。

注: 模 2 除法的具体过程参考 CRC 校验理论部分。

试题 4 答案

(4) B

试题 5 分析

海明码是一种纠错码, 不但能发现差错, 而且还能纠正差错。对于 m 位数据, 增加 k 位冗余位, 若满足关系式: $m+k+1 < 2^k$, 则可以纠正 1 位错。

试题 5 答案

(5) A

6.4 考前冲刺

试题 1

假设模拟信号的最高频率为 5MHz, 如果每个样本量化为 256 个等级, 则传输的数据速率是 (1)。

- (1) A. 10Mb/s B. 50Mb/s C. 80Mb/s D. 100Mb/s

试题 2

采用 CRC 校验的生成多项式为 $G(x)=x^{16}+x^{15}+x^2+1$, 它产生的校验码是 (2) 位。

- (2) A. 2 B. 4 C. 16 D. 32

试题 3

关于曼彻斯特编码, 下面叙述中错误的是 (3)。

- (3) A. 曼彻斯特编码是一种双相码
B. 采用曼彻斯特编码, 波特率是数据速率的 2 倍
C. 曼彻斯特编码可以自同步
D. 曼彻斯特编码效率高

试题 4

E1 信道的数据速率是 (4)。

- (4) A. 1.544Mb/s B. 2.048Mb/s C. 6.312Mb/s D. 44.736Mb/s

试题 5

假设模拟信号的最高频率为 5MHz, 采样频率必须大于 (5), 才能使得到的样本信号不失真。

- (5) A. 5MHz B. 10MHz C. 15MHz D. 20MHz

试题 6

在以太网中使用 CRC 校验码, 其生成多项式是 (6)。

- (6) A. $G(x)=x^{16}+x^{12}+x^5+1$
B. $G(x)=x^{16}+x^{15}+x^2+1$

C. $G(x)=x^{12}+x^{11}+x^3+x^2+x+1$

D. $G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^3+x+1$

试题 7

在异步通信中, 每个字符包含 1 位起始位、7 位数据位、1 位奇偶校验位和 1 位终止位, 每秒钟传送 100 个字符, 则有效数据速率为 (7)。

- (7) A. 500b/s B. 600b/s C. 700b/s D. 800b/s

试题 8

采用 CRC 进行差错校验, 生成多项式为 $G(x)=x^4+x+1$, 信息码字为 10110, 则计算出的 CRC 校验码是 (8)。

- (8) A. 0000 B. 0100 C. 0010 D. 1111

试题 9

采用海明码进行差错校验, 信息码字为 1001011, 为纠正一位错, 则需要 (9) 比特冗余位。

- (9) A. 2 B. 3 C. 4 D. 8

试题 10

曼彻斯特编码的特点是在每个比特的中间有电平翻转, 它的编码效率是 (10)。

- (10) A. 50% B. 60% C. 80% D. 100%

试题 11

4B/5B 编码是一种两级编码方案, 首先要把数据变成 (11) 编码, 再把 4 位分为一组的代码转换成 5 单位的代码。

- (11) A. NRZ-I B. AMI C. QAM D. PCM

试题 12

图 6-18 表示了某个数据的两种编码, 这两种编码分别是 (12)。

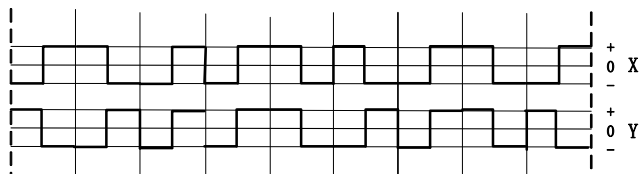


图 6-18 两种编码波形

- (12) A. X 为差分曼彻斯特码, Y 为曼彻斯特码
B. X 为差分曼彻斯特码, Y 为双极性码
C. X 为曼彻斯特码, Y 为差分曼彻斯特码
D. X 为曼彻斯特码, Y 为不归零码

试题 13

图 6-19 所示的调制方式是 (13)。

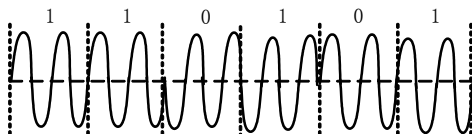


图 6-19 某种调制方式波形

- (13) A. FSK B. 2DPSK C. ASK D. QAM

试题 14

图 6-20 所示的调制方式是 2DPSK，若载波频率为 2400Hz，则码元速率为 (14)。

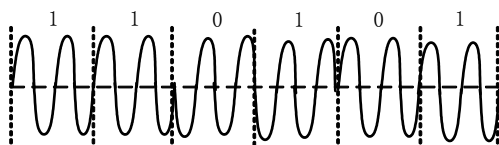


图 6-20 2DPSK 调制方式波形

- (14) A. 100 Baud B. 200 Baud C. 1200 Baud D. 2400 Baud

试题 15

在相隔 2000km 的两地间通过电缆以 4800b/s 的速率传送 3000 比特长的数据包，从开始发生到接收数据需要的时间是 (15)。

- (15) A. 480ms B. 645ms C. 630ms D. 635ms

试题 16

在地面上相隔 2000km 的两地之间通过卫星信道传送 4000 比特长的数据包，如果数据速率为 64kb/s，则从开始发送到接收完成需要的时间是 (16)。

- (16) A. 48ms B. 640ms C. 322.5ms D. 322.5ms

试题 17

下面关于 Manchester 编码的叙述中，错误的是 (17)。

- (17) A. Manchester 编码是一种双相码
B. Manchester 编码提供了比特同步信息
C. Manchester 编码的效率为 50%
D. Manchester 编码应用在高速以太网中

试题 18

设信道采用 2DPSK 调制，码元速率为 300 波特，则最大数据速率为 (18) b/s。

- (18) A. 300 B. 600 C. 900 D. 1200

试题 19

10BASE-T 以太网使用曼彻斯特编码，其编码效率为 (19)%。在快速以太网中使用 4B/5B 编码，其编码效率为 (21)%。

- (19) A. 30 B. 50 C. 80 D. 90
(20) A. 30 B. 50 C. 80 D. 90

试题 20

SDH 同步数字体系是光纤信道的复用标准，其中最常用的 STM-1 (OC-3) 的数据速率是 (21)，STM-4 (OC-12) 的数据速率是 (22)。

- (21) A. 155.520Mb/s B. 622.080Mb/s
C. 2488.320Mb/s D. 10Gb/s
(22) A. 155.520Mb/s B. 622.080Mb/s
C. 2488.320Mb/s D. 10Gb/s

6.5 习题解析

试题 1 分析

按照尼奎斯特采样定理, 为了恢复原来的模拟信号, 取样速率必须大于模拟信号最高频率的二倍, 即

$$f = \frac{1}{T} > 2f_{\max}$$

其中 f 为采样频率, T 为采样周期, f_{\max} 为模拟信号的最高频率。所以当模拟信号的频率为 5MHz 时, 采样频率必须大于 10MHz。

当样本量空间被量化为 256 个等级时, 每个样本必须用 8 比特来表示。根据计算:

$$8 \times 10\text{MHz} = 80\text{Mb/s}$$

试题 1 答案

(1) C

试题 2 分析

循环冗余校验码 CRC (Cyclic Redundancy Check) 的长度取决于生成多项式的幂次。如果生成多项式为 $G(x) = x^{16} + x^{15} + x^2 + 1$, 则产生的 CRC 校验码必定是 16 位。

试题 2 答案

(2) C

试题 3 分析

双相码的特点是每一位中都有一个电平转换, 因而这种代码的最大优点是自定时。曼彻斯特编码是一种双相码, 通常用高电平到低电平的转换边表示 0, 用低电平到高电平的转换边表示 1, 相反的规定也是可能的。位中间的电平转换边既表示了数据代码, 也作为定时信号使用。曼彻斯特编码用在 10M 以太网中。差分曼彻斯特编码也是一种双相码, 与曼彻斯特编码不同的是, 位中间的电平转换只作为定时信号, 而不表示数据。数据的表示在于每一位开始处是否有电平转换: 有电平转换表示 0, 无电平转换表示 1。差分曼彻斯特编码用在令牌环网中。

曼彻斯特编码和差分曼彻斯特编码的每一个码元都要调制为两个不同的电平, 因而调制速率是码元速率的两倍, 也就是说编码效率只有 50%。这无疑对信道的带宽提出了更高的要求, 但由于良好的抗噪声特性和自定时能力, 所以在局域网中仍被广泛使用。

试题 3 答案

(3) D

试题 4 分析

国际电报电话咨询委员会于 1993 年后改为 ITU-T, 建议了一种 PCM 传输标准, 称为 E1 载波。该标准规定, 每一帧开始处用 8 位作为同步位, 中间有 8 位信令位, 再组织 30 路 8 位数据 (可传送语音), 全帧包括 256 位, 每一帧用 125 μ s 时间传送。可计算出 E1 载波的数据速率为 $256\text{b}/125\mu\text{s} = 2.048\text{Mb/s}$, 每个语音信道的数据速率为 $8\text{b}/125\mu\text{s} = 64\text{Kb/s}$ 。

试题 4 答案

(4) B

试题 5 分析

按照尼奎斯特采样定理, 为了恢复原来的模拟信号, 取样速率必须大于模拟信号最高频

率的二倍，即

$$f = \frac{1}{T} > 2f_{\max}$$

其中 f 为采样频率， T 为采样周期， f_{\max} 为模拟信号的最高频率。所以当模拟信号的频率为 5MHz 时，采样频率必须大于 10MHz。

试题 5 答案

(5) B

试题 6 分析

为了能对不同的错误模式进行校验，已经研究出了几种 CRC 生成多项式的国际标准如下。

CRC-CCITT $G(x)=x^{16}+x^{12}+x^5+1$

CRC-16 $G(x)=x^{16}+x^{15}+x^2+1$

CRC-12 $G(x)=x^{12}+x^{11}+x^3+x^2+x+1$

CRC-32 $G(x)=x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^3+x+1$

其中 CRC-32 用在以太网中，这种生成多项式能产生 32 位的帧校验序列。

试题 6 答案

(6) D

试题 7 分析

异步通信以字符为传送单位，每个字符添加一个起始位和终止位。按照题中给出的条件，可计算如下：

$$\frac{7}{1+7+1+1} \times 100 = 700\text{b/s}$$

试题 7 答案

(7) C

试题 8 分析

循环冗余校验码的计算方法如下。

$G(x)=x^4+x+1$ 对应的二进制序列为 10011，下面进行“按位异或”运算：

101100000

10011

0010100

10011

0011100

10011

01111

1111 就是校验码。

试题 8 答案

(8) D

试题 9 分析

按照海明的理论，纠错编码就是要把所有合法的码字尽量安排在 n 维超立方体的顶点上，使得任一对码字之间的距离尽可能大。如果任意两个码字之间的海明距离是 d ，则所有

少于等于 $d-1$ 位的错误都可以检查出来，所有少于 $d/2$ 位的错误都可以纠正。

如果对于 m 位的数据，增加 k 位冗余位，则组成 $n=m+k$ 位的纠错码。对于 2^m 个有效码字中的每一个，都有 n 个无效但可以纠错的码字。这些可纠错的码字与有效码字的距离是 1，含单个错。这样，对于一个有效的消息总共有 $n+1$ 个可识别的码字。这 $n+1$ 个码字相对于其他 2^{m-1} 个有效消息的距离都大于 1。这意味着总共有 $2^m(n+1)$ 个有效的或是可纠错的码字。显然，这个数应小于等于码字的所有可能的个数 2^n 。于是，有 $2^m(n+1) \leq 2^n$ 。

因为 $n=m+k$ ，可得出 $m+k+1 \leq 2^k$ 。对于给定的数据位 m ，上式给出了 k 的下界，即要纠正单个错误， k 必须取的最小值。根据上式计算，可得 $7+k+1 \leq 2^k$ ，所以 $k=4$ 。

试题 9 答案

(9) C

试题 10 分析

曼彻斯特编码 (Manchester Code) 是一种双相码 (或称分相码)。双相码要求每一位中间都要有一个电平转换，因而这种代码的优点是自定时，同时双相码也有检测差错的功能，如果某一位中间缺少了电平翻转，则被认为是违例代码。我们用高电平到低电平的转换边表示“0”，而低电平到高电平的转换边表示“1”，相反的表达也是允许的。比特中间的电平转换既表示了数据代码，同时也作为定时信号使用。曼彻斯特编码用在以太网中。

差分曼彻斯特编码类似于曼彻斯特编码，它把每一比特的起始边有无电平转换作为区分“0”和“1”的标志，这种编码用在令牌环网中。

在曼彻斯特编码和差分曼彻斯特编码中，每比特中间都有一次电平跳变，因此波特率是数据速率的两倍。对于 100Mb/s 的高速网络，如果采用这类编码方法，就需要 200M 的波特率，其编码效率为 50%。

试题 10 答案

(10) A

试题 11 分析

采用 4B/5B 编码能够提高编码的效率，降低电路成本。这种编码方法的原理如图 6-21 所示。

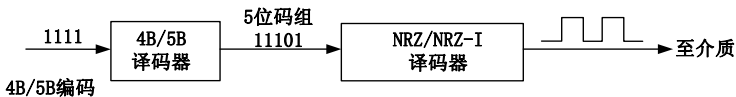


图 6-21 4B/5B 编码原理

这实际上是一种两级编码方案。系统中使用不归零码 (NRZ)，在发送到传输介质时变成 1 就翻不归零码 (NRZ-1)。NRZ-1 代码序列中 1 的个数越多，越能提供同步信息，如果遇到长串的“0”，则不能提供同步信息，所以在发送到介质上之前还需经过一次 4B/5B 编码。发送器扫描要发送的位序列，4 位分为一组，然后按照对应规则变换成 5 位二进制代码。

5 位二进制代码的状态共有 32 种，其中 1 的个数都不少于 2 个，这样就保证了传输的代码能提供足够多的同步信息。

试题 11 答案

(11) A

试题 12 分析

首先可以断定图中所示是两种双相码，然后按照曼彻斯特编码的特点 (以正负或负正脉

冲来区别“1”和“0”)和差分曼彻斯特编码的特点(以位前沿是否有电平跳变来区别“1”和“0”)可以断定, X 为曼彻斯特编码, Y 为差分曼彻斯特编码。

试题 12 答案

(12) B

试题 13 分析

根据波形可以看出, 这是一种差分编码, 所以应选 2DPSK。

试题 13 答案

(13) B

试题 14 分析

2DPSK 调制方式波形中, 每一位包含两个周期, 如果载波频率为 2400Hz, 则码元速率就是 1200 波特。

试题 14 答案

(14) C

试题 15 分析

一个数据包从开始发送到接收完成的时间包含发送时间 t_f 和传播延迟时间 t_p 两部分, 可以计算如下:

对电缆信道: $t_p=2000\text{km}/(200\text{km/ms})=10\text{ms}$, $t_f=3000\text{b}/4800\text{b/s}=625\text{ms}$, $t_p+t_f=635\text{ms}$ 。

试题 15 答案

(15) D

试题 16 分析

卫星通信一般是指同步卫星通信, 同步卫星距地球约 3.6 万公里, 电磁波一个来回约 270ms, 从开始发送到接收完成需要的时间=发送时间+卫星信道延时时间=4000/64+270=62.5+270=332.5ms。这里要注意 2000km 这个干扰信息, 因为只要是卫星通信, 不管在地球上相隔多远, 他们的通信延时都是要经过先发送到卫星, 再从卫星返回这么一个过程。

试题 16 答案

(16) D

试题 17 分析

本题考查数据编码的基础知识。

Manchester 编码是一种双相码, 即码元取正负两个不同的电平, 或者说由正负两个不同的码元表示一个比特, 这样编码的效率为 50%, 但是由于每个比特中间都有电平跳变, 因而提供了丰富的同步信息。这种编码用在数据速率不太高的以太网中。

差分 Manchester 编码也是一种双相码, 但是区分“0”和“1”的方法不同。Manchester 编码正变负表示“0”, 负变正表示“1”, 而差分 Manchester 编码是“0”比特前沿有跳变, “1”比特前沿没有跳变。这种编码用在令牌环网中。

在曼彻斯特和差分曼彻斯特编码中, 每比特中间都有一次电平跳变, 因此波特率是数据速率的两倍。对于 100Mb/s 的高速网络, 如果采用这类编码方法, 就需要 200M 的波特率, 其硬件成本是 100M 波特率硬件成本的 5~10 倍。

试题 17 答案

(17) D

试题 18 分析

本题考查数字调制的基础知识。2DPSK 是一种差分相位调制技术, 利用前后码元之间的相位变化来表示二进制数据, 例如传送“1”时载波相位相对于前一码元的相移为 π , 传送“0”时载波相位相对于前一码元的相移为 0。在这种调制方案中, 每一码元代表一个比特, 由于码元速率为 300 波特, 所以最大数据速率为 300b/s。

试题 18 答案

(18) A

试题 19 分析

使用曼彻斯特编码和差分曼彻斯特编码时, 每传输 1bit 的信息, 就要求线路上有 2 次电平状态变化 (2 Baud), 因此要实现 100Mb/s 的传输速率, 就需要有 200MHz 的带宽, 即编码效率只有 50%。正是因为曼码的编码效率不高, 因此在带宽资源宝贵的广域网, 以及速度要求更高的局域网中, 就面临了困难。因此就出现了 $mBnB$ 编码, 也就是将 m 比特位编码成为 n 波特 (代码位)。其中 4B/5B 效率为 80%。

试题 19 答案

(19) B

(20) C

试题 20 分析

SDH 的速率是一个必须记住的知识点, SDH 是通信技术中的传输技术, 是目前骨干网及接入网中使用最广的传输技术。其基本传输单元是 STM-1, 上有 SMT-4、STM-16 和 STM-64 等, 都是 4 倍的关系。STM-1 的传输速率是 155.520Mb/s。

其中 STM-1 光接口数据速率是 155Mb/s, STM-4 是 622Mb/s, STM-16 是 2.5Gb/s, STM-64 是 10Gb/s, 其中 STM-1 对应 OC-3, STM-4 对应 OC-12。

试题 20 答案

(21) A

(22) B

局域网（Local Area Network, LAN）是在一个局部的地理范围内（如一个学校、工厂和机关内），一般是方圆几千米以内，将各种计算机，外部设备和数据库等互相连接起来组成的计算机通信网。它可以通过数据通信网或专用数据电路，与远方的局域网、数据库或处理中心相连接，构成一个较大范围的信息处理系统。局域网可以实现文件管理、应用软件共享、打印机共享、扫描仪共享、工作组内的日程安排、电子邮件和传真通信服务等功能。局域网严格意义上是封闭型的，它可以由办公室内几台甚至上千上万台计算机组成。决定局域网的主要技术要素为：网络拓扑、传输介质与介质访问控制方法。

7.1 考点脉络

数据通信基础是网络工程师考试的非常重要的一个考点。

根据考试大纲，要求考生掌握以下几个方面的内容。

- （1）传输介质和网络设备：包括双绞线、光纤等介质和交换机、路由器等设备。
- （2）综合布线系统：包含六大子系统的名称、位置、设备等。
- （3）以太网技术：包括帧结构、CSMA/CD 等知识点。
- （4）WLAN 技术：包括无线局域网标准、组网方式。
- （5）虚拟局域网：包括 VLAN 划分、trunk 技术等知识点。

从历年的考试试题来看，本章的考点在综合知识考试中的平均分数为 9 分，约为总分的 12%。考试试题分数主要集中在 CSMA/CD、无线局域网标准和组网方式、VLAN 技术这 3 个知识点上。

7.2 介质、网络设备、综合布线系统

在介质、设备、综合布线系统这个考点中，主要涉及双绞线、光纤介质的特点、交换机工作原理、路由器工作原理、综合布线系统这 4 方面的内容。

7.2.1 考点精讲

双绞线和光纤介质是目前在网络中使用最广的物理传输介质，作为网工方向学员应该熟知其基本的特征。

交换机是数据链路层核心设备，数据帧的交换是其基本功能。如果是三层交换机，则会有三层的路由转发功能。

路由器是最重要的网络互联设备，其基本功能是子网划分、路由等。

综合布线系统是为了顺应发展需求而特别设计的一套布线系统。对于现代化的大楼来

说，就如体内的神经，它采用了一系列高质量的标准材料，以模块化的组合方式，把语音、数据、图像和部分控制信号系统用统一的传输媒介进行综合，经过统一的规划设计，综合在一套标准的布线系统中，将现代建筑的三大子系统有机地连接起来，为现代建筑的系统集成提供了物理介质。可以说结构化布线系统的成功与否直接关系到现代化的大楼的成败，选择一套高品质的综合布线系统是至关重要的。

1. 网络传输介质

对于本知识点来说，主要是要求能够了解各种常见的传输介质的特性，如最大传输距离、数据传输速率等，以及它们之间的横向比较。不过值得注意的是，在网络工程师考试下午模块中，通常在第一大题中，也还是会有一些与传输介质相关的问题（例如：在网络拓扑中，如何选择适当的传输介质），这就要求考生对常见传输介质的特性、性价比有综合考虑。

(1) 综合比较

计算机网络中可以使用各种传输介质来组成物理信道，根据其形态可以分为有线传输介质和无线传输介质两大类，表 7-1 列出了有线传输介质的主要知识点。

表 7-1 有线传输介质及其特性

传 输 介 质	类 型	距 离	速 度	特 点
同轴电缆	细缆 RG58	185m	10Mb/s	安装容易，成本低，抗干扰性较强
	粗缆 RG11	500m	10Mb/s	安装较难，成本低，抗干扰性强
	粗缆 RG59	>10km	100~150Mb/s	传输模拟信号（CATV），也叫宽带同轴电缆，常使用 FDM（频分多路复用）
屏蔽双绞线（STP）	3 类/5 类	100m	16/100Mb/s	相对于 UTP 笨重，令牌环网常用，现在 7 类布线系统又开始使用
无屏蔽双绞线(UTP)	3/4/5/超 5/6 类	100m	16/20/100/155/200Mb/s	价格便宜，安装容易，适用于结构化综合布线，随着网卡技术的发展，在短距离内甚至可以达到 1Gb/s
光纤	多模	550m	100~1000Mb/s	电磁干扰小，数据速度高，误码率小，低延迟
	单模	5km	1~10Gb/s	与多模光纤比，特点是：高速度、长距离、高成本、细芯线，常使用 WDM（波分复用）提高带宽

无线传输介质主要包括无线电波、微波和红外线。

- ① 无线电波：需要专用的频率，易被窃听。
- ② 微波：可分为地面微波和卫星微波，带宽高、容量大，但受天气影响大。
- ③ 红外线：设备便宜、带宽高，但传输距离有限，易受室内空气状态影响。

以太网比较常用的传输介质包括同轴电缆（已淘汰，不再介绍）、双绞线、光纤三种。以太网命名格式按照 N-信号-物理介质的格式。格式中每个元素都有其固定的含义，具体如下。

N：以兆位为单位的数据速率，如 10、100、1000。

信号：基带还是宽带。

物理介质：标识介质类型。

用 10Base-T 来举例，如图 7-1 所示。

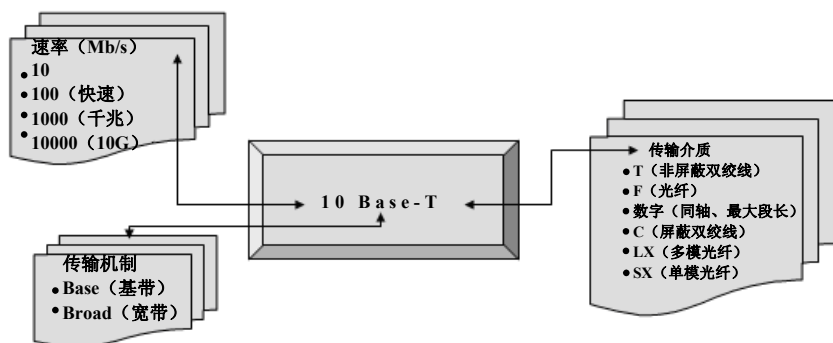


图 7-1 以太网传输介质标识

(2) 双绞线的物理特性

双绞线包括如下几种物理特性。

① 衰减：衰减是沿链路的信号损失度量。衰减与线缆的长度相关，随着长度的增加，信号衰减也随之增加。衰减用分贝 dB 作为单位，表示源传送端信号到接收端信号强度的比率。

② 近端串扰：当电流在一条导线中流通时，会产生一定的电磁场，干扰相邻导线上的信号。频率越高这种影响就越大。双绞线就是利用两条导线绞合在一起后，因为相位相差 180° 的原因而抵消相互间的干扰的。绞距越紧则抵消效果越佳，也就越能支持较高的数据传输速率。

③ 直流电阻：直流环路电阻会消耗一部分的信号，并将其转变成热量。它是指一对导线电阻的和。

④ 特性阻抗：与环路直流电阻不同，特性阻抗包括电阻及频率为 $1\sim 100\text{MHz}$ 的电感阻抗，它与一对电线间的距离及绝缘体的电气性能有关。

⑤ 衰减串扰比 (ACR)：它由最差的衰减量与 NEXT 量值的差值计算出。ACR 值较大时，表示抗干扰的能力更强。一般要求大于 10dB 。

(3) 光纤特性

按传输点模数分类可以分为单模光纤 (Single-mode Fiber, SMF) 和多模光纤 (Multi-mode Fiber, MMF)。

① SMF 的纤芯直径很小，在给定的工作波长上只能以单一模式传输，传输频带宽，传输容量大。由于 SMF 的纤芯直径非常细小，价格昂贵。

② MMF 是在给定的工作波长上，能以多种模式同时传输的光纤。模式色散会使多模光纤的带宽变窄，降低了其传输容量，因此 MMF 仅适用于较小容量的光纤通信。与单模光纤相比，MMF 的传输性能较差。

从工作的波长来分，可分为以下两类。

① 短波长光纤：光波之波长在 $0.6\sim 0.9\mu\text{m}$ 范围内，典型值为 $0.85\mu\text{m}$ ，习惯上把在此波长范围内呈现低衰耗的光纤称作短波长光纤。

② 长波长光纤：人们的研究工作迅速转移，并研制出衰耗更低、带宽更宽的光纤，习惯上把工作在此 $1.0\sim 2.0\mu\text{m}$ 波长范围的光纤称为长波长光纤。

2. 网络设备

对于本知识点来说，本部分的知识重点在于了解中继器、网桥、路由器、网关、交换机

等常见互联设备的特性及应用领域、设备工作的层次、冲突域与广播域的划分。

(1) 互联设备

常见的网络互联设备包括中继器、网桥、路由器和网关。以上是从 OSI 协议层出发的概念分类，实际上，市场上的设备都是多功能组合的。例如，应用广泛、功能各异的集线器、交换机，其实它们只是以上 4 种基本设备的一种特殊形式。表 7-2 则是对以上设备的一个总结。

表 7-2 网络互联设备

互 联 设 备	工 作 层 次	主 要 功 能
中继器	物理层	对接收信号进行再生和发送，只起到扩展传输距离作用，对高层协议是透明的，但使用个数有限（以太网是 4 个）
网桥	数据链路层	根据帧物理地址进行网络间信息转发，可缓解网络通信繁忙度，提高效率。一般用于连接具有相同 MAC 层的网络
路由器	网络层	通过逻辑地址进行网络间信息转发，可完成异构网络之间的互联互通，只能连接使用相同网络层协议的子网
网关	高层（4~7）	最复杂的网络互联设备，用于连接网络层上执行不同协议的子网（例如 Novell 与 SNA）
集线器	物理层	多端口中继器
二层交换机	数据链路层	多端口网桥
三层交换机	网络层	带路由功能的二层交换机
多层交换机	高层（4~7）	带协议转换的交换机

通常网桥（包括二层交换机）用于局域网互联，而路由器常用于广域网互联。三层交换机则应用于局域网/城域网中不同逻辑子网（网络层）的互联。

(2) 交换机与多层交换

交换机根据其工作的原理，可以分为二层、三层、多层等。

① 二层交换机与网桥的比较

网桥在应用时存在着以下不足：无路由功能；容易产生广播包，可能会导致广播风暴；可能会造成数据包的循环问题；在某些情况下，因网桥拥塞而丢失帧，使网络不稳定、不可靠。

二层交换技术从网桥发展到 VLAN（虚拟局域网），它按照所接收到数据包的目的 MAC 地址来进行转发，对于网络层或者高层协议来说是透明的。它不处理网络层的逻辑地址，可处理物理地址（MAC 地址），数据交换是靠硬件来实现的，速度相当快。

注：总线带宽应超过“端口数×端口带宽”才能够实现线速交换。交换机的 MAC 地址表大小将影响交换机的接入容量。

② 三层交换机与路由器的比较

为了解决网桥的缺点，引入了路由器设备。但路由器是无连接的设备，而且要对每个数据包进行“拆装”，导致路由器吞吐量有限，容易成为网络瓶颈。路由器的转发效率要比二层低。而三层交换技术的出现，使得既利用了二层转发效率高的优点，又实现了处理三层 IP 数据包的能力。

第三层交换技术也称为 IP 交换技术、高速路由技术等，第三层交换技术实质上是路由，即“路由一次，交换多次”的基于高性能硬件的线速路由器。

③ 多协议标记交换

多协议标记交换（MPLS）是将第二层交换功能与第三层路由功能结合在一起的技术，

在 IP 路由和控制协议的基础上, MPLS 提供了面向连接的交换, 也属于三层交换技术。由于 MPLS 可以支持多种网络层的协议 (包括 IPv4、IPv6、IPX、CLNP 等), 同时还支持第二层的各种协议, 而并不是针对某一种链路的技术, 因此称之为多协议。MPLS 使用的是固定长度的短标记作为数据转发的依据。

④ 高层交换技术

除了二层交换、三层交换和 MPLS 交换之外, 还有四层交换、七层交换等高层交换技术。第四层交换的简单定义是: 可以不仅依据 MAC 地址 (第二层网桥) 或源/目标 IP 地址 (第三层路由), 而且依据 TCP/UDP (第四层) 应用端口号决定传输。第四层交换的功能可以归纳为以下 5 个方面。

a. 第四层交换可以根据应用进行流量排队, 这为基于规则的服务质量机制提供了一条可操作的途径。

b. 第四层交换提供了以应用为基础配置网络的工具。

c. 第四层交换提供附加的硬件手段来以每端口为基础收集应用层流量统计。

d. 第四层交换技术从头至尾跟踪和维持各个会话, 是真正的“会话交换机”。

e. 第四层交换技术主要可用于“负载均衡”。

七层交换机则能够智能化地进一步控制, 对所有传输流和内容进行控制。由于可以自由地完全打开传输流的应用/表示层, 仔细分析其中的内容, 因此可以根据应用的类型而非仅仅根据 IP 和端口号做出更智能的决定。它也可以实现有效的数据流优化和智能负载均衡。

(3) 交换机的堆叠与级联

① 堆叠: 是通过厂家提供的一条专用连接电缆, 从一台交换机的“UP”堆叠端口直接连接到另一台交换机的“DOWN”端口, 以实现单台设备端口数的扩充。其作用就像一个模块化交换机一样, 堆叠在一起的交换机可以当作一个单元设备来进行管理。

② 级联: 是在网络中增加节点数的另一种方法, 级联既可使用普通端口也可使用特殊的 Uplink 口和 MDI 端口。当相互级联的两个端口分别为普通端口和 MDI 端口或 Uplink 端口时, 应当使用直通电缆。当相互级联的两个端口均为普通端口或 Uplink 端口或 MDI 端口时, 则应当使用交叉电缆。

(4) 路由器与链路汇聚

路由器的端口主要分局域网端口、广域网端口和配置端口三类。

① 局域网端口

a. AUI 端口: 就是用来与粗同轴电缆连接的接口, 路由器可通过粗同轴电缆收发器实现与 10Base-5 网络的连接。

b. RJ-45 端口: 双绞线以太网端口。根据端口的通信速率不同, RJ-45 端口又可分为 10Base-T、100Base-TX 和 1000Base-T 三类。其中, 10Base-T 端口在路由器中通常标识为 ETH 或 Ethernet, 而 100Base-TX 端口则通常标识为 10/100bTX 或 FastEthernet, 千兆位端口通常被标记为 GE。

c. 光纤端口: 光纤端口有 SC 和 LC 两种类型, 用于与光纤的连接。光纤端口通常不直接用光纤连接至工作站, 而是通过光纤连接到快速以太网或千兆以太网等具有光纤端口的交换机、路由器或其他远程网络设备。

② 广域网端口

a. RJ-45 端口: 利用 RJ-45 端口也可以建立广域网与 VLAN (虚拟局域网) 之间, 以及

与远程网络或 Internet 的连接。

b. 高速同步串口：“高速同步串口”(SERIAL)，主要用于连接目前应用非常广泛的 DDN、帧中继 (Frame Relay)、X.25、PSTN (模拟电话线路) 等网络连接模式。在企业网之间有时也通过 DDN 或 X.25 等广域网连接技术进行专线连接。

c. 异步串口：主要应用于 Modem 或 Modem 池的连接，实现远程计算机通过公用电话网拨入网络。这种接口所连接的通信方式速率较低。

d. ISDN BRI 端口：用于 ISDN 线路通过路由器实现与 Internet 或其他远程网络的连接，可实现 128Kb/s 的通信速率。ISDN 有两种速率连接端口，一种是 ISDN BRI (基本速率接口)；另一种是 ISDN PRI (基群速率接口)。

③ 路由器配置端口

路由器的配置端口有两个，分别是 Console 和 AUX。Console 通常用来进行路由器的基本配置时通过专用连线与计算机连接用的，初始配置时必须使用此接口。而 AUX 是用于路由器的远程配置连接的。

a. Console 端口：使用配置专用连线直接连接至计算机的串口，利用终端仿真程序（如 Windows 下的“超级终端”）进行路由器本地配置。

b. AUX 端口：异步端口，主要用于远程配置，也可用于拨号连接，还可通过收发器与 Modem 进行连接。

链路汇聚 (Trunk) 也称为端口汇聚、端口捆绑、链路扩容组合，即两台设备之间通过两个以上的同种类型的端口进行连接，同时传输数据，以便提供更高的带宽、更好的冗余度以及实现负载均衡，如图 7-2 所示。

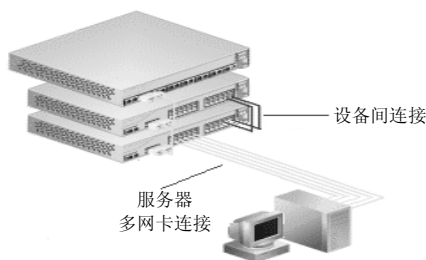


图 7-2 链路汇聚

链路汇聚是一种封装技术，它是一条点到点的链路，链路的两端可以都是交换机，也可以是交换机和路由器，还可以是主机和交换机或路由器。它能够为设备间提供连接的高速通道。它通过配置软件的设置，将几个物理端口组合成一个逻辑端口，将属于这几个端口的带宽合并，给端口提供一个 $N \times 2 \times$ 单个端口带宽的独享的高带宽。

Trunk 功能比较适合于以下方面的具体应用。

① 与服务器相连，给服务器提供独享的高带宽。

② 与网络设备之间的级联，通过牺牲端口数来给设备之间的数据交换提供捆绑的高带宽，提高网络速度，突破网络瓶颈，进而大幅度提高网络性能。

③ 可以提供负载均衡能力以及系统容错。由于 Trunk 实时平衡各个设备端口和服务器接口的流量，一旦某个端口出现故障，它会自动把故障端口从 Trunk 组中撤销，进而重新分配各个 Trunk 端口的流量，从而实现系统容错。

(5) 冲突域与广播域

冲突域与广播域的示意图如图 7-3 所示。

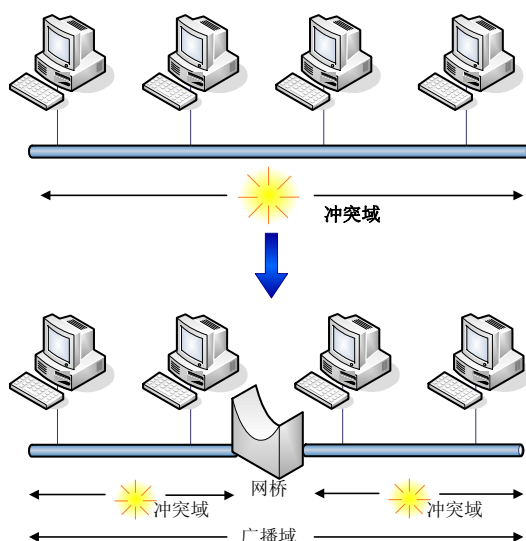


图 7-3 冲突域与广播域示意图

从图 7-3 中我们可以看出，“冲突域”是指会发生物理碰撞的域，可以通过加入第二层桥接技术或交换技术来进行逻辑分段，即可解决，也就是“用交换机/网桥解决介质争用问题”；但逻辑分段并没有分解“广播域”，要分解广播域需要使用第三层设备（即路由器或三层交换机）。

① 中继器、集线器：单纯地放大传播信号，运行在物理层，不能划分广播域和冲突域。

② 网桥、二层交换机：运行在数据链路层，可划分冲突域，不可划分广播域。

③ 路由器、网关、三层交换机、多层交换机：运行在网络层，可划分冲突域和广播域。

其中，前两项增加了冲突域的数量，减少了冲突域的范围；最后一项增加了广播域的数量，减少了广播域的范围，划分子网就属于此类。

3. 综合布线系统

本知识点重点在于掌握综合布线技术的基础概念，能够知道 6 个子系统的作用、特点，并且能够在实际的组网过程中，正确地选择相应的设备与介质。

如图 7-4 所示，整个综合布线系统通常由工作区子系统、水平子系统、干线子系统、设备间子系统、管理子系统和建筑群主干子系统 6 个部分组成。

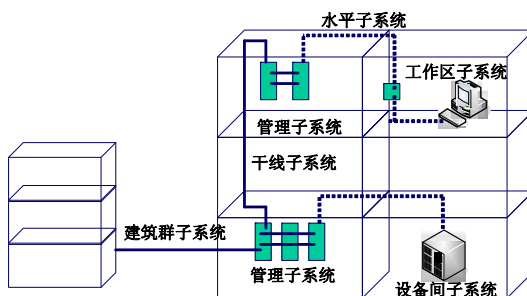


图 7-4 综合布线系统的组成

(1) 工作区子系统：是连接用户终端设备的子系统，主要包括信息插座、信息插座和设备之间的适配器。通俗地说，就是指计算机和网线接口之间的部分。

(2) 水平子系统：是连接工作区与主干的子系统，主要包括配线架、配线电缆和信息插座。通俗地说，就是指从楼层弱电井里的配线架到每个房间的网卡接口之间的部分，通常布线是在天花板上，因此与楼层平行。在水平子系统中，使用的是星型拓扑，即将每个网卡接口（信息模块）接回配线架，每个口一根线。

(3) 管理子系统：管理子系统是对布线电缆进行端接及配置管理的子系统，通常在各个楼层都会设立。通俗地讲，这就是配线间中的设备部分。

(4) 干线子系统：是用来连接管理间、设备间的子系统。通俗地说，就是将接入层交换机连接到分布层（或核心层）交换机的网络线路，由于其通常是顺着大楼的弱电井而下，是与大楼垂直的，因此也称为垂直子系统。通常来说，干线经常使用光缆，另外高品质的 5 类/超 5 类以及 6 类非屏蔽双绞线也是十分常用的。

(5) 设备间子系统：是安装在设备间的子系统，而设备间是指集中安装大型设备的场所。一般来说，大型建筑物都会有一个或多个设备间。通常核心交换机所在的位置就是设备间。它与管理子系统相比，对于物理环境的要求更高。

(6) 建筑群主干子系统：它是用来连接楼群之间的子系统，包括各种通信传输介质和支持设备，由于在户外，因此又称为户外子系统。通常包括地下管道、直埋沟内、架空三种方式。现在许多新的建筑物，通常都会预先留好地下管道。

7.2.2 一点一练

试题 1

图 7-5 的网络配置中，总共有 (1) 个广播域，(2) 个冲突域。

- (1) A. 2 B. 3 C. 4 D. 5
(2) A. 2 B. 5 C. 6 D. 10

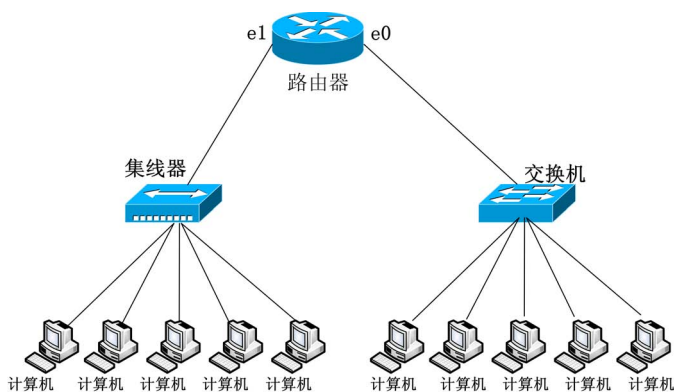


图 7-5 某拓扑图

试题 2

多协议标记交换（MPLS）是 IETF 提出的第三层交换标准，下面有关 MPLS 的描述中，正确的是 (3)。

- (3) A. MPLS 支持各种网络层协议，带有 MPLS 标记的分组必须封装在 PPP 帧中传送
B. MPLS 标记在各个子网中是特定分组的唯一标识
C. 路由器可以根据转发目标把多个 IP 流聚合在一起，组成一个转发等价类（FEC）
D. 传送带有 MPLS 标记的分组之前先要建立对应的网络连接

试题 3

布线实施后需要进行测试,在测试线路的主要指标中,__(4)__是指一对相邻的线通过电磁感应所产生的耦合信号。

- (4) A. 近端串扰 B. 衰减值 C. 回波损耗 D. 传输延迟

试题 4

布线实施后需要进行测试,在测试线路的主要指标中,__(5)__是由于集肤效应、绝缘损耗、阻抗不匹配、连接电阻等因素,造成信号沿链路传输时的损失。

- (5) A. 近端串扰 B. 衰减值 C. 回波损耗 D. 传输延迟

试题 5

通常情况下,信息插座的安装位置距离地面的高度为__(6)__cm。

- (6) A. 10~20 B. 20~30 C. 30~50 D. 50~70

试题 6

某 IP 网络连接如图 7-6 所示,在这种配置下 IP 全局广播分组不能够通过的路径是__(7)__。

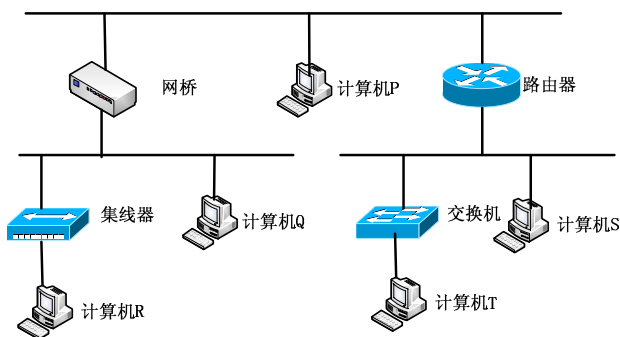


图 7-6 网络连接拓扑图

- (7) A. 计算机 P 和计算机 Q 之间的路径 B. 计算机 P 和计算机 S 之间的路径
C. 计算机 Q 和计算机 R 之间的路径 D. 计算机 S 和计算机 T 之间的路径

试题 7

以太网交换机是按照__(8)__进行转发的。

- (8) A. MAC 地址 B. IP 地址 C. 协议类型 D. 端口号

试题 8

快速以太网标准 100BASE-TX 采用的传输介质是__(9)__。

- (9) A. 同轴电缆 B. 无屏蔽双绞线 C. CATV 电缆 D. 光纤

试题 9

路由器的 S0 端口连接__(10)__。

- (10) A. 广域网 B. 以太网 C. 集线器 D. 交换机

试题 10

关于路由器,下列说法中错误的是__(11)__。

- (11) A. 路由器可以隔离子网,抑制广播风暴
B. 路由器可以实现网络地址转换
C. 路由器可以提供可靠性不同的多条路由选择

D. 路由器只能实现点对点的传输

7.2.3 解析与答案

试题 1 分析

本题考查广播域、冲突域概念。

在网络内部,数据分组产生和发生冲突的这样一个区域被称为冲突域。所有的公共介质环境都是冲突域。一条线路可通过接插电缆、收发器、接插面板、中继器和集线器与另一条线路进行连接。所以这些第一层的互联设备都是冲突域的一部分。

广播数据包会在交换机连接的所有网段上传播,在某些情况下会导致通信拥挤和安全漏洞。连接到路由器上的网段会被分配成不同的广播域,广播数据不会穿过路由器。传统的交换机只能分割冲突域,不能分割广播域。要隔离广播域需要采用第三层的设备,如路由器,所以图 7-5 中共有 2 个广播域。

集线器是共享式,属于 1 个冲突域,而交换机由于不是共享式,其每个端口是一个冲突域,但整个交换机属于一个广播域,除非采用 vlan 的技术可以对广播进行隔离。所以,冲突域=集线器的冲突域+交换机的冲突域=1+5=6。

试题 1 答案

(1) A (2) C

试题 2 分析

有 MPLS 标记的分组不但可以封装在 PPP 帧中传送,还可以封装在以太网、ATM 和帧中继中。MPLS 标记具有局部性,一个标记只是在一定的传输域中有效。以太网传输数据帧,没有什么建立连接的概念。

试题 2 答案

(3) C

试题 3 分析

通常,双绞线系统的测试指标主要集中在链路传输的最大衰减值和近端串音衰减等参数上。

近端串扰(NEXT):类似于噪声,是从相邻的一对线上传过来的干扰信号。这种串扰信号是由于 UTP 中,邻近的线对通过电容和电感耦合过来的。

试题 3 答案

(4) A

试题 4 分析

通常,双绞线系统的测试指标主要集中在链路传输的最大衰减值和近端串音衰减等参数上。

衰减(Attenuation):指信号沿链路传输的减弱。链路传输的最大衰减值是由于集肤效应、绝缘损耗、阻抗不匹配、连接电阻等因素,造成信号沿链路传输损失的能量。

试题 4 答案

(5) B

试题 5 分析

通常,信息插座的安装位置距离地面的高度为 30~50cm。

试题 5 答案

(6) C

试题 6 分析

在主干网上，路由器的主要作用是路由选择。主干网上的路由器，必须知道到达所有下层网络的路径。这需要维护庞大的路由表，并对连接状态的变化做出尽可能迅速的反应。路由器的故障将会导致严重的信息传输问题。

在园区网内部，路由器的主要作用是分隔子网。随着网络规模的不断扩大，局域网演变成以高速主干和路由器连接的多个子网所组成的园区网。在其中，各个子网在逻辑上独立，而路由器就是唯一能够分隔它们的设备，它负责子网间的报文转发和广播隔离，在边界上的路由器则负责与上层网络的连接。

交换机只能缩小冲突域，而不能缩小广播域。整个交换式网络就是一个大的广播域，广播报文散到整个交换式网络。而路由器可以隔离广播域，广播报文不能通过路由器继续进行广播。P 和 S 被 Router 隔开，属于不同的广播域。

A 答案中，P、Q 中间有二层设备 Bridge，不在同一个冲突域当中，但在同一个广播域中。

C 答案中，Q、R 中间只有一个一层设备 Hub，既在同一个广播域中，也在同一个冲突域中。

D 答案中，S、T 中间有二层设备 Switch，不在同一个冲突域当中，但在同一个广播域中。

因此，备选答案中只有计算机 P 和计算机 S 之间的路径 IP 全局广播分组不能够通过。

试题 6 答案

(7) B

试题 7 分析

以太网交换机是按照 MAC 地址进行转发的。交换机识别以太帧中的目标地址，选择对应的端口把以太帧转发出去。

试题 7 答案

(8) A

试题 8 分析

快速以太网标准 100BASE-TX 采用的传输介质是 5 类无屏蔽双绞线（UTP），TX 表示 Twisted Pair。

试题 8 答案

(9) B

试题 9 分析

路由器的 S0 端口连接广域网，如图 7-7 所示。

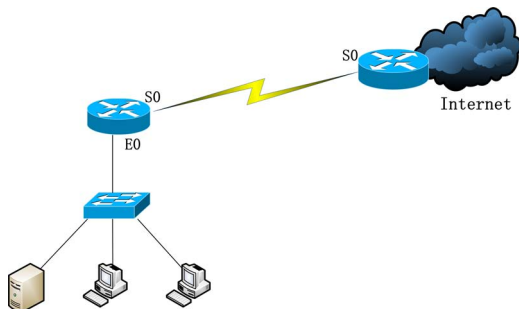


图 7-7 路由器 S0 端口连接示意图

试题 9 答案

(10) A

试题 10 分析

路由器是网络层设备，它可以起到隔离子网、抑制广播风暴的作用。路由器还能进行地址转换，通常用于把私有地址转换成公网地址，或者进行相反的转换。在路由表中，对于同一目标，可以设置不同的通路，提供不同的服务。IPv4 数据报头的第二个字节是服务类型字段（Type of Service）。该字段规定了不同的优先级（Precedence）、延迟（Delay）、吞吐率（Throughput）和可靠性（Reliability），为上层协议提供不同的服务质量。IP 数据报中的目标地址（Destination address）字段可以是广播地址、组播地址和单播地址，当目标地址为前两种类型时，路由器可以实现点到多点的传输。

试题 10 答案

(11) D

7.3 以太网技术和无线局域网

在以太网技术和无线局域网这个考点中，主要涉及 CSMA/CD、无线局域网这两方面的内容。

7.3.1 考点精讲

CSMA/CD 是以太网中最常见的介质访问控制机制。

无线局域网在当今企业的网络架构中普遍存在，它是对有线局域网的一种延伸。

1. 以太网技术

对于本知识点来说，主要要求了解 IEEE 802 系列标准、LLC 与 MAC 协议、CSMA/CD 协议等知识。

(1) IEEE 802 标准

本知识点重点在于 IEEE 802 下属的 12 个分委员会所对应的标准，内容如下所示。

802.1：局域网概念、体系结构、网络管理和性能测量等。

802.2：逻辑链路控制协议（LLC）。

802.3：以太网的介质访问控制协议（CSMA/CD）及物理层技术规范。

802.4：令牌总线网介质访问控制协议及其物理层技术规范。

802.5：令牌环网访问控制协议及其物理层技术规范。

802.6：城域网介质访问控制协议 DQDB 及其物理层技术规范。

802.7：宽带技术咨询组。

802.8：光纤技术咨询组。

802.9：综合语音/数据的局域网（IVD LAN）介质访问控制协议以及物理层技术规范。

802.10：局域网安全技术标准。

802.11：无线局域网的介质访问控制协议及其物理层技术规范。

802.12：100Mb/s 高速以太网按需优先的介质访问控制协议 100VG-Any LAN。

以太网传输技术与编码技术的对应关系如表 7-3 所示。

表 7-3 以太网传输技术与编码技术的对应关系

传输技术	100Base-T	1000Base-T	100Base-TX	1000Base-LX	1000Base-SX	1000Base-CX	10GBase-T
编码技术	PAM-5	PAM-5	4B/5B	8B/10B	8B/10B	8B/10B	PAM-10

(2) LLC 与 MAC 协议

由于局域网使用了多种传输介质，而介质访问协议又与具体的传输介质和拓扑结构相关，所以 IEEE 802 标准将数据链路层分成了两个子层：一个是与物理介质相关的部分，称为介质访问控制子层（MAC）；另一个是统一的逻辑链路控制子层（LLC）。

① 辑链路控制子层

LLC 协议能够提供 3 种服务，如表 7-4 所示。

表 7-4 LLC 三种服务类型

服 务 类 型	特 点	适 用 性	LLC 操作类型
无确认无连接的服务	数据报类型，不涉及任何流控与差错控制功能	一是高层软件具有流控和差错控制；二是连接建立和维护机制引起了不必要的开销	LLC1 型操作：用无编号信息帧支持无连接服务
面向连接方式的服务	类似于 HDLC，在数据通信前需要建立连接，同时通过连接来提供流控和差错控制功能	可用于简单设备中，如终端控制器，它自身流控差，需要借助数据链路层协议	LLC2 型操作：用 HDLC 的异步平衡方式的操作支持连接方式的 LLC 服务
有确认无连接的服务	它提供了数据报确认功能，但不建立连接	它高效、可靠，适合于传送少量的重要数据	LLC3 型操作：用两种新的无编号帧支持有确认无连接服务

② 介质访问控制子层

根据介质访问控制的方式，可以将 MAC 分为循环、预约和竞争 3 种方式，在几种主要的 MAC 协议中都使用了不同的方式，如表 7-5 所示。

表 7-5 介质访问控制方式

方 式	特 点	应 用
循环式	每个站轮流得到发送机会。如果一段时间内有許多站发数据，则该方式很有效；如果有很少站发数据，则该方式的开销太大	令牌总线 令牌环 FDDI
预约式	将传输介质的使用时间划分为时间槽，而预约管理可以是集中控制，也可以是分布控制	DQDB
竞争式	不对各个工作站的发送权限进行控制，而是自由竞争，它适于分布式控制，优点在于简单，轻负载下效率高，重负载时效率下降很快	CSMA/CD

(3) CSMA/CD 协议

本知识点重点在于理解 CSMA/CD，掌握 3 种监听算法、冲突窗口的计算以及计算冲突检测所需的传播时延。

IEEE 802.3 标准所采用的 CSMA/CD（载波监听多路访问/冲突检测）协议对于总线、星型和树型拓扑结构是最合适的介质访问控制协议，它属于竞争式介质访问控制协议。

① 波监听

冲突虽然没有办法避免，但是可以通过精心设计的监听算法来缓解，各种算法如表 7-6 所示。

表 7-6 载波监听算法

监 听 算 法	信 道 空 闲 时	信 道 忙 时	特 点
非坚持型监听算法	立即发送	等待 N，再监听	减少冲突，信道利用率降低
1-坚持型监听算法	立即发送	继续监听	提高信道利用率，增大了冲突
P-坚持型监听算法	以概率 P 发送	继续监听	有效平衡，但复杂

注：非坚持型监听算法的 N 可取任意随机值，在 P-坚持型监听算法中，信道空闲将以概率 $(1-P)$ 延迟一个时间单位（该时间单位为网络传输时延期 τ ）。

② 冲突检测

载波监听只能够减少冲突的概率，但无法完全避免冲突。为了能够高效地实现冲突检测，在 CSMA/CD 中采用了边发送边听的冲突检测方法。也就是由发送者一边发，一边自己接收回来，一旦发现结果出现不同，马上停止发送，并发出冲突信号，这时所有的站都会收到阻塞信息，并都等待一段时间之后再重新监听。而等待的这段时间的长度对网络的稳定工作有很大影响，常用的策略是“二进制指数后退算法”，算法如下：

a. 对每个帧，当第一次发生冲突时，设置参量为 $L=2$ 。

b. 退避间隔取 $1 \sim L$ 个时间片中的一个随机数，1 个时间片等于 $2a$ （双向传播时间 $=2a$ ，即 $a=0.5$ ）。

c. 当帧重复一次冲突时，则将参量 L 加倍。

d. 设置一个最大重传次数，超过这个次数，则不再重传，并报告出错。

正是因为采用了边发边听的检测方法，因此检测冲突所需要花的最长时间是网络传播延迟的两倍（最大段长/信号传播速度，这是对于基带系统而言的，有些宽带系统需要网络传播延迟的 4 倍时间才够），这称之为冲突窗口。因此，为了保证在信息发送完成之前能够检测到冲突，发送的时间应该大于等于冲突窗口，这也就规定了最小的帧长 $=2 \times (\text{网络数据速率} \times \text{最大段长} / \text{信号传播速度})$ 。

③ 性能分析

a. 吞吐率 (T)：单位时间内实际传送的位数。

$$T = \text{帧长} / (\text{网络段长} / \text{传播速度} + \text{帧长} / \text{网络数据速率})$$

b. 网络利用率 (E)：

$$E = \text{吞吐率} / \text{网络数据速率}$$

另外，802.3 的 MAC 帧结构中有几个小知识点还需要了解。以太网帧结构如图 7-8 所示。

其中帧头中有源地址和目标地址字段，存放着 MAC 地址，通常是 6 字节长（48 位），IEEE 为每个硬件制造商指定了网卡的 MAC 地址的前 3 字节，后 3 字节则由制造商编码。目标地址首位为 0，则代表普通地址；如果首位为 1，则说明是组播地址；地址全 1，则代表广播地址。802.3 的最大帧长为 1564 字节（最大的数据帧为 1500 字节），最小帧长为 64 字节，如果不足则需要加入填充位。



图 7-8 以太网帧结构

2. 令牌环网

本知识点重点在于理解令牌的工作原理，了解 MAC 帧结构、物理层规范，监控站的功能，掌握网络所需的最小时延值、影响因素及相关计算方法。

令牌环网采用的不是广播介质，而是使用中继器将单个的点到点线路链接成为物理的环形结构，然后通过令牌这种特殊的控制帧来进行传输的管理。令牌环的 MAC 帧有两种结构，一是令牌帧（只有表示帧开始、结束的边界字段，以及访问控制字段），另一个是数据帧。令牌环网的帧是支持优先级设置的，也是采用 CRC32 进行帧头校验的，并且对帧长没有任何限制。

令牌环网数据帧格式与令牌格式如图 7-9 所示。

环的长度往往折算成比特数来衡量，以比特度量的环长反映了环上能容纳的比特数量。环上每个中继器可引入一位或几位延时。把环看作一个环缓冲器，则有：
环上的比特数=传播延时×发送介质长度×数据传输速率+中继器延迟

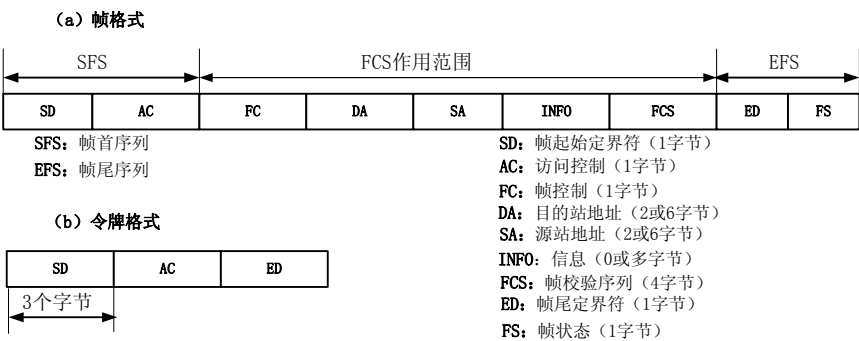


图 7-9 令牌环网数据帧格式与令牌格式

3. 无线局域网

本知识点重点在于掌握 802.11 的 4 个标准，了解它们的频段、主要技术、速度，熟悉基础设施网络和 Ad Hoc 两种组网形式，熟悉 WLAN 的具体应用以及 RADIUS 登录的基础知识。

(1) 802.11 标准系列

IEEE 802.11 先后提出了以下多个标准，最早的 802.11 标准只能达到 1~2Mb/s 的速度，在制定更高速度的标准时，就产生了 802.11a 和 802.11b 两个分支，后来又推出了 802.11g 的新标准，如表 7-7 所示。

表 7-7 无线局域网标准

标 准	运 行 频 段	主 要 技 术	数 据 速 率
802.11	2.4GHz 的 ISM 频段	扩频通信技术	1Mb/s 和 2Mb/s

续表

标 准	运 行 频 段	主 要 技 术	数 据 速 率
802.11b	2.4GHz 的 ISM 频段	CCK 技术	11Mb/s
802.11a	5GHz U-NII 频段	OFDM 调制技术	54Mb/s
802.11g	2.4GHz 的 ISM 频段	OFDM 调制技术	54Mb/s

注：ISM 是指可用于工业、科学、医疗领域的频段；U-NII 是指用于构建国家信息基础的无限制频段。

IEEE 802.11a、IEEE 802.11b 或 IEEE 802.11g，主要是以物理层的不同作为区分，所以它们的区别直接表现在工作频段以及数据传输速率、最大传输距离这些指标上。而工作在媒介层的标准又分 IEEE 802.11h、IEEE 802.11e、IEEE 802.11i、IEEE802.11n 几种标准。

802.11h 是 802.11a 的扩展，目的是兼容其他 5GHz 频段的标准，如欧盟使用的 HyperLAN2。

802.11e 是 IEEE 为满足服务质量（QoS）方面的要求而制定的 WLAN 标准。在一些对时间敏感、有严格要求的业务（如语音、视频等）中，QoS 是非常重要的指标。在 802.11 MAC 层，802.11e 加入了 QoS 功能，其中的混合协调功能可以单独使用或综合使用以下两种信道接入机制：一种是基于论点式的（Contentionbased），一种是基于投票式的（Polled）。

IEEE 802.11i 规定使用 802.1x 认证和密钥管理方式，在数据加密方面，定义了 TKIP（Temporal Key Integrity Protocol）、CCMP（Counter-Mode/CBC-MAC Protocol）和 WRAP（Wireless Robust Authenticated Protocol）三种加密机制。其中 TKIP 采用 WEP 机制里的 RC4 作为核心加密算法，可以通过在现有的设备上升级固件和驱动程序的方法达到提高 WLAN 安全的目的。CCMP 机制基于 AES 加密算法和 CCM（Counter-Mode/CBC-MAC）认证方式，使得 WLAN 的安全程度大大提高，是实现 RSN 的强制性要求。由于 AES 对硬件要求比较高，因此，CCMP 无法通过在现有设备的基础上进行升级实现。WRAP 机制基于 AES 加密算法和 OCB（Offset Codebook），是一种可选的加密机制。

802.11n 主要是结合物理层和 MAC 层的优化来充分提高 WLAN 技术的吞吐。主要的物理层技术涉及了 MIMO、MIMO-OFDM、40MHz、Short GI 等技术，从而将物理层吞吐提高到 600Mb/s。

在传输速率方面，802.11n 可以将 WLAN 的传输速率由目前 802.11a 及 802.11g 提供的 54Mb/s，提高到 300Mb/s 甚至高达 600Mb/s。得益于将 MIMO（多入多出）与 OFDM（正交频分复用）技术相结合而应用的 MIMO OFDM 技术，提高了无线传输质量，也使传输速率得到极大提升。

在覆盖范围方面，802.11n 采用智能天线技术，通过多组独立天线组成的天线阵列，可以动态调整波束，保证让 WLAN 用户接收到稳定的信号，并可以减少其他信号的干扰。因此其覆盖范围可以扩大到好几平方公里，使 WLAN 移动性极大提高。

在兼容性方面，802.11n 采用了一种软件无线电技术，它是一个完全可编程的硬件平台，使得不同系统的基站和终端都可以通过这一平台的不同软件实现互通和兼容，这使得 WLAN 的兼容性得到极大改善。这意味着 WLAN 将不但能实现 802.11n 向前后兼容，而且可以实现 WLAN 与无线广域网络的结合，比如 3G。

（2）WLAN 组网方式

在 802.11 的标准提案中，规定了两种工作模式，分别是有接入点（Access Point，AP，访问点、基站）模式（基础设施网络）和无访问点模式（Ad Hoc 网络）。其结构如图 7-10

所示。

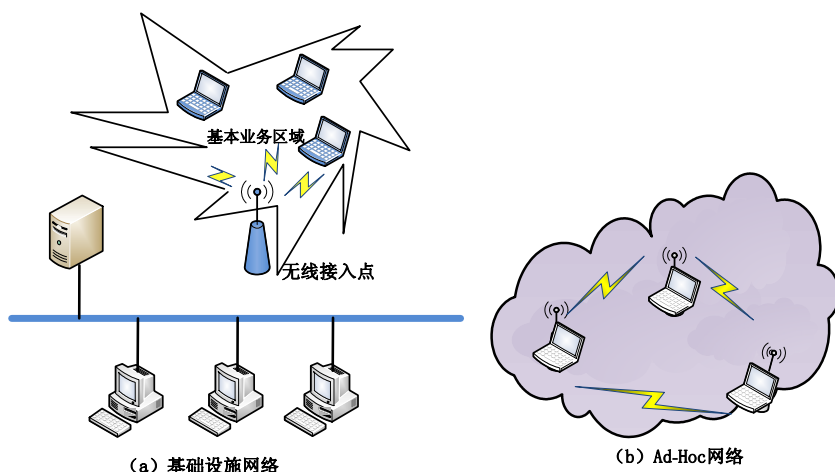


图 7-10 两种 WLAN 网络拓扑

① 基础设施网络：它需要通过接入点（AP）来访问骨干网，或互相访问。它的作用与网桥类似，负责在 802.11 和 802.3 的 MAC 协议之间进行转换。一个接入点覆盖的部分称为一个基本业务域（BSA），而接入点控制的所有终端组成一个基本业务集（BSS），由两个以上的 BSA 可以组成一个分布式系统（DS）。

② Ad Hoc 网络：不使用接入点，直接通过无线网卡实现点对点连接。和基础设施网络相比，它的可扩展性和灵活性更好，但是路由、协调控制等技术都难以解决。

（3）WLAN 物理层和服务

WLAN 物理层规定了使用的传输技术，服务规定了 WLAN 所提供的功能。

① 物理层

802.11 使用了 5 种传输技术。

a. 红外：使用 0.85 或 0.95 μm 波段上的漫射传输，允许 1Mb/s 或 2Mb/s 的速率，它无法穿过墙壁，带宽低，不是很通用的方案。

b. FHSS（跳频扩频）：短距离的无线电波，使用了 79 个 1MHz 的信道，抗干扰能力强，主要缺点是带宽低。

c. DSSS（直接序列扩频）：也是短距离的无线电波，也被限制在 2Mb/s 的速率上。

d. OFDM（正交频分多路复用）：可以达到 54Mb/s，频谱效率高，抗干扰性强。

e. HR-DSSS（高速率的直接序列扩频）：可达到 11Mb/s，称为 802.11b。它的覆盖范围可以是 OFDM 的 7 倍。

② 服务

服务包括 5 种分发服务和 4 种站服务。分发服务涉及对单元的成员关系的管理，并且会影响单元外的站；而站服务则只与一个单元内部的活动有关系。5 种分发服务是由 AP 提供的，它们处理站的移动性，进入单元时进行关联，离开单元时断开联系。

a. 关联：移动站利用该服务连接到 AP 上。

b. 分离：移动站离开或关闭时解除关联关系。

c. 重新关联：改变其首选 AP。

d. 分发：决定如何路由那些发送给 AP 的帧。

e. 融合：使用非 802.11 的网络发送信息。

而内部单元则包括 4 种站服务。

a. 认证：在 WLAN 中，每一个站都必须证明自己的身份才能够发送数据。整个过程如图 7-11 所示。

b. 解除认证：已经通过认证的移动站要离开网络时，就需要解除认证。

c. 私密性：当 WLAN 需要对发送的信息保密时，可以使用该服务，指定的加密算法是 RC4。

e. 数据投递：即数据的传输功能。

结合以上文字，我们来看看 AP 与移动站之间的认证过程，如图 7-11 所示。

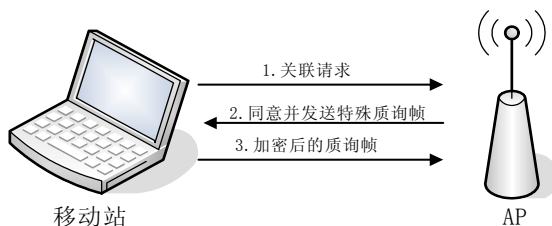


图 7-11 移动站认证过程示意图

注：如果 AP 收到正确的加密帧，就说明其知道预先分配的口令。

(4) WLAN 安装与配置

首先，安装无线网络的核心——AP，由于它的作用是将有线网络的信息转化为无线信号，因此它的位置决定了整个无线网络的信号强度和传输速率。然后，对 AP 进行如下相关配置。

① 输入 AP 的管理员密码 SSID（也被称为 ESSID 或 Network Name），它用来标识不同的无线网络信号。然后根据 AP 的预设 IP 地址和掩码，设置客户端的 IP 地址与掩码，这样打开 AP 后，无线网卡就能够自行找到，就可以测试无线连接是否正常。

② 使用 AP 的配置界面设置 IP 分配方式，它提供了“静态分配”和“动态分配”两种方式，建议使用动态分配方式。

③ 最后，配置安装加密功能。由于在默认情况下，AP 是不加密的，因此连接成功后应该对 AP 的配置界面（通常是 Web 式界面）进行修改。802.11b 无线网络最常用的加密手段是 WEP。

a. 配置 AP：在 AP 配置界面的“安全”选项中，打开“WEP”加密功能，然后输入一段十六进制的字符（字符必须为 0~9 及 A~F）作为加密字串，这个字串一定要记牢，遗失后将无法连接 AP），保存设置后重新启动 AP。而这个加密字串的位数取决于 WEP 类型，如果采用 64 位加密，则需要输入 10 位的加密字串；如果是 128 位加密，则需要输入 26 位的加密字串。

b. 配置客户端：在无线网卡的“属性”项中，将“数据加密（Web 启用）”这一项激活，然后在“网络密钥（encryption）”和“确认网络密钥”两项中填入在 AP 上设置的加密字串。

(5) 设置 RADIUS

RADIUS 主要用于对远程拨入的用户进行授权和认证。它可以仅使用单一的“数据库”

对用户进行认证（校验用户名和口令）。在使用 RADIUS 验证时，整个过程如下。

① 客户端发送一个“Access-Request”数据包给 RADIUS 服务器，其中包含了用户名、口令（使用 MD5 加密）、ID 号和用户访问的端口号。如果 RADIUS 服务器在规定时间内没有访问，则会重发；如果有多个 RADIUS 服务器，则会在多次尝试连接主 RADIUS 服务器失败后，转向使用其他 RADIUS 服务器。

② RADIUS 服务器收到“Access-Request”包后，会在认证数据库中查找用户是否存在，如果存在，则提取此用户的信息列表，其中包括了用户的口令、访问端口和访问权限，并根据该信息进行验证。

如果信息被否认，则返回“Access-Reject”数据报，指示此用户非法，还将根据需要返回错误信息。如果信息被确认，则发送“Access-Challenge”数据报给客户端，并加入状态属性等反馈信息。

注：RADIUS 服务器会直接抛弃没有加“共享密钥”的请求。而对于无法满足的请求，会转给其他 RADIUS 服务器。

③ 客户端收到“Access-Challenge”包后，就会再次提交带新请求 ID 的“Access-Request”数据报，其内容与最初的不同之处在于：“用户名/口令”信息替换为加密信息，加上了“Access-Challenge”的状态属性。

④ 如果所请求的合法，RADIUS 服务器返回一个“Access-Accept”数据报，其中包括了服务类型（可以是 SLIP、PPP、Login User）及相关信息。例如，PPP 中就包括 IP 地址、子网掩码、MTU 和数据报过滤标识等。

归纳一下，一个成功的 RADIUS 登录过程，一般包括两次握手的过程：首先发送一个实时的 Access-Request 数据报，带上用户名、口令、访问端口信息，请求验证；RADIUS 服务器通过查询认证数据库鉴权通过后，返回 Access-Challenge 应答包询问具体的访问请求，并带上状态属性与相关信息；客户端收到后，则用 Access-Challenge 包中的信息组成新的 Access-Request 数据报；最后服务器应答 Access-Accept 包，完成验证登录过程。图 7-12 显示了这个过程。

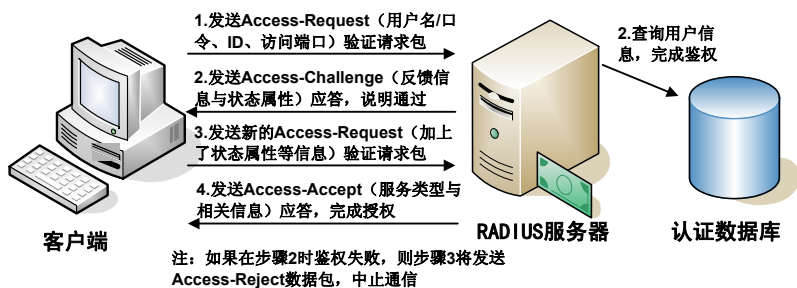


图 7-12 RADIUS 登录过程示意图

7.3.2 一点一练

试题 1

在无线局域网 802.11 标准体系中，802.11n 能够达到的最大理论值为____(1)____。

- (1) A. 11Mb/s B. 54Mb/s C. 2Mb/s D. 600Mb/s

试题 2

在 802.11 定义的各种业务中，优先级最低的是____(2)____。

- (2) A. 分布式竞争访问 B. 带应答的分布式协调功能

C. 服务访问节点轮询

D. 请求/应答式通信

试题 3

802.11b 定义了无线网的安全协议 WEP (Wired Equivalent Privacy)。以下关于 WEP 的描述中, 正确的是____(3)_____。

- (3) A. 采用的密钥长度是 80 位
B. 其加密算法属于公开密钥密码体系
C. WEP 只是对 802.11 站点之间的数据进行加密
D. WEP 也可以保护 AP 有线网络端的数据安全

试题 4

IEEE 802.3ae 10Gb/s 以太网标准支持的工作模式是____(4)_____。

- (4) A. 全双工
B. 半双工
C. 单工
D. 全双工和半双工

试题 5

以太网的数据帧封装如图 7-13 所示, 包含在 TCP 段中的数据部分最长应该是____(5)_____字节。

目的MAC地址	源MAC地址	协议类型	IP头	TCP头	数据	CRC
---------	--------	------	-----	------	----	-----

图 7-13 以太帧格式

- (5) A. 1434 B. 1460 C. 1480 D. 1500

试题 6

下列关于 1000BaseT 的叙述中错误的是____(6)_____。

- (6) A. 可以使用超 5 类 UTP 作为网络传输介质
B. 最长有效距离可以达到 100 米
C. 支持 8B/10B 编码方案
D. 不同厂商的超 5 类系统之间可以互用

试题 7

在以太网中, 最大传输单元 (MTU) 是____(7)_____字节。

- (7) A. 46 B. 64 C. 1500 D. 1518

试题 8

光纤布线系统的测试指标不包括____(8)_____。

- (8) A. 最大衰减限值 B. 波长窗口参数 C. 回波损耗限值 D. 近端串扰

试题 9

802.11 标准定义了 3 种物理层通信技术, 这 3 种技术不包括____(9)_____。

- (9) A. 直接序列扩频 B. 跳频扩频 C. 窄带微波 D. 漫反射红外线

试题 10

802.11 标准定义的分布式协调功能采用了____(10)_____协议。

- (10) A. CSMA/CD B. CSMA/CA C. CDMA/CD D. CDMA/CA

7.3.3 解析与答案

试题 1 分析

802.11n 主要是结合物理层和 MAC 层的优化来充分提高 WLAN 技术的吞吐。主要的物

理层技术涉及了 MIMO、MIMO-OFDM、40MHz、Short GI 等技术，从而将物理层吞吐提高到 600Mb/s。

在传输速率方面，802.11n 可以将 WLAN 的传输速率由目前 802.11a 及 802.11g 提供的 54Mb/s，提高到 300Mb/s 甚至高达 600Mb/s。得益于将 MIMO（多入多出）与 OFDM（正交频分复用）技术相结合而应用的 MIMO OFDM 技术，提高了无线传输质量，也使传输速率得到极大提升。

试题 1 答案

(1) D

试题 2 分析

IEEE 802.11MAC 子层定义了 3 种访问控制机制：CSMA/CA、RTS/CTS 和点协调功能。CSMA/CA 类似于 802.3 的 CSMA/CD 协议，这种访问控制机制叫做载波监听多路访问/冲突避免协议。分布式协调功能（Distributed Coordination Function，DCF）利用了 CSMA/CA 协议，在此基础上又定义了点协调功能（Point Coordination Function，PCF）。DCF 是数据传输的基本方式，作用于信道竞争期，PCF 工作于非竞争期。两者总是交替出现，先由 DCF 竞争介质使用权，然后进入非竞争期，由 PCF 控制数据传输。

为了使各种 MAC 操作互相配合，IEEE 802.11 推荐使用 3 种帧间隔（IFS），以便提供基于优先级的访问控制。

DIFS（分布式协调 IFS）：最长的 IFS，优先级最低，用于异步帧竞争访问的时延。

PIFS（点协调 IFS）：中等长度的 IFS，优先级居中，在 PCF 操作中使用。

SIFS（短 IFS）：最短的 IFS，优先级最高，用于需要立即响应的操作。

DIFS 用在 CSMA/CA 协议中，只要 MAC 层有数据要发送，就监听信道是否空闲。如果信道空闲，等待 DIFS 时段后开始发送；如果信道忙，就继续监听，直到可以发送为止。

IEEE 802.11 还定义了带有应答帧(ACK)的 CSMA/CA。AP 收到一个数据帧后等待 SIFS 再发送一个应答帧 ACK。由于 SIFS 比 DIFS 小得多，所以其他终端在 AP 的应答帧传送完成后才能开始新的竞争过程。

PCF 是在 DCF 之上实现的一个可选功能。所谓点协调就是由 AP 集中轮询所有终端，为其提供无竞争的服务，这种机制适用于时间敏感操作。轮询过程中使用 PIFS 作为帧间隔时间。由于 PIFS 比 DIFS 小，所以点协调能够优先 CSMA/CA 获得信道，并把所有的异步帧都推后传送。

试题 2 答案

(2) A

试题 3 分析

IEEE 802.11 提供的加密方法采用 WEP（Wired Equivalent Privacy）标准。WEP 对数据的加密和解密都使用同样的算法和密钥。它包括“共享密钥”认证和数据加密两个过程。认证过程采用了标准的询问和响应帧式。在执行过程中，AP 根据 RC4 算法运用共享密钥对 128 字节的随机序列进行加密后作为询问帧发给用户，用户将收到的询问帧进行解密后以正文形式响应 AP，AP 将正文与原始随机序列进行比较，如果两者一致，则通过认证。

如果用户激活了 WEP，无线网卡就对 802.11 帧的负载进行加密，则接收站则对收到的帧进行解密。所以 WEP 只是对 802.11 站点之间的数据进行加密。一旦帧进入了有线网络，WEP 就不起作用了。也就是说 WEP 不支持端到端的加密和认证。

WEP 标准说明了共享的 40 或 64 位密钥，某些制造商的产品则把密钥扩展到 128 位（有

时称为 WEP 2)，每一个无线网卡和访问点必须配置同样的密钥才能互相通信。

试题 3 答案

(3) C

试题 4 分析

万兆以太网具有全双工的工作模式：万兆位以太网只在光纤上工作，并只能在全双工模式下操作，这意味着不必使用冲突探测协议，因此它本身没有距离限制。它的优点是减少了网络的复杂性，兼容现有的局域网技术并将其扩展到广域网，同时有望降低系统费用，并提供更快、更新的数据业务。

万兆以太网可继续在局域网中使用，也可用于广域网中，而这两者之间工作环境不同。不同的应用环境对于以太网各项指标的要求存在许多差异，针对这种情况，人们制定了两种不同的物理介质标准。这两种物理层的共同点是共用一个 MAC 层，仅支持全双工，省略了带冲突检测的载波侦听多路访问（Carrier Sense Multiple Access with Collision Detection，CSMA/CD）策略，采用光纤作为物理介质。

试题 4 答案

(4) A

试题 5 分析

在早些时候，以太网的数据帧最大长度是 1518 个字节，不包括前同步码和帧开始定界符，格式如图 7-14 所示。

目的MAC地址	源MAC地址	协议类型	IP头	TCP头	数据	CRC
---------	--------	------	-----	------	----	-----

图 7-14 以太帧格式

其中目标 MAC 地址占 6 个字节，源 MAC 地址占 6 个字节，协议类型占 2 个字节，IP 头最小 20 字节，TCP 头最小 20 字节，CRC 占 4 个字节。因此 TCP 段中的数据部分的最大长度应该是 $1518-6-6-2-20-20-4=1460$ 。

试题 5 答案

(5) B

试题 6 分析

1000BaseT 是一种使用 5 类 UTP 作为网络传输介质的千兆以太网技术，最长有效距离与 100BaseTX 一样可以达到 100 米。可以采用这种技术在原有的快速以太网系统中实现从 100Mb/s 到 1000Mb/s 的平滑升级。与前面所介绍的其他三种网络介质不同，1000BaseT 不支持 8B/10B 编码方案，需要采用专门的更加先进的编码/译码机制。

试题 6 答案

(6) C

试题 7 分析

在以太网中，最大传输单元（MTU）是 1500 个字节，最大帧长是 1518 个字节。

试题 7 答案

(7) C

试题 8 分析

由于在光纤系统的实施过程中，涉及光纤的镞铺设，光纤的弯曲半径，光纤的熔接、跳

线,更由于设计方法及物理布线结构的不同,导致两网络设备间的光纤路径上光信号的传输衰减有很大不同。虽然光纤的种类较多,但光纤及其传输系统的基本测试方法大体相同,所使用的测试仪器也基本相同。对磨接后的光纤或光纤传输系统,必须进行光纤特性测试,使之符合光纤传输通道测试标准。基本的测试内容包括如下三方面:

① 波长窗口参数

综合布线系统光纤波长窗口的各项参数,应符合有关规定。

② 光纤布线链路的最大衰减限值

综合布线系统的光纤布线链路的衰减限值,应符合有关规定。

③ 光回波损耗限值

综合布线系统光纤布线链路任一接口的光回波损耗限值,应符合有关规定。

试题 8 答案

(8) D

试题 9 分析

IEEE 802.11 标准定义了 3 种物理层通信技术:直接序列扩频、跳频扩频、漫反射红

外线。

试题 9 答案

(9) C

试题 10 分析

IEEE 802.11 标准定义的分布式协调功能采用了载波监听多路访问/冲突避免(CSMA/CA 协议)。在无线网中进行冲突检测是有困难的。例如两个站由于距离过大或者中间障碍物的分隔而检测不到冲突,但是位于它们之间的第三个站可能会检测到冲突,这就是所谓隐蔽终端问题。采用冲突避免的办法可以解决隐蔽终端的问题。802.11 定义了一个帧间隔(Inter Frame Spacing, IFS)时间。另外还有一个后退计数器,其初始值是由随机数发生器设置的,递减计数直到 0。基本的操作过程如下。

① 如果一个站有数据要发送并且监听到信道忙,则产生一个随机数设置自己的后退计数器并坚持监听。

② 监听到信道空闲后等待一个 IFS 时间,然后开始计数,最先计数完的站可以开始发送。

③ 其他站在监听到有新的站开始发送后暂停计数,在新的站发送完成后再等待一个 IFS 时间继续计数,直到计数完成开始发送。

CSMA/CA 协议可以采用载波检测方法发现信道空闲,也可以采用能量检测方法发现信道空闲。这个算法对参与竞争的站是公平的,基本上是按先来先服务的顺序获得发送的机会。

试题 10 答案

(10) B

7.4 虚拟局域网

虚拟局域网这一考点中,主要涉及 VLAN 的划分和配置、VTP、STP 三方面的内容。

7.4.1 考点精讲

虚拟局域网(Virtual Local Area Network, VLAN)是一种将局域网设备从逻辑上划分成一个个网段,从而实现虚拟工作组的新兴数据交换技术。这一新兴技术主要应用于交换机和路由器中,但主流应用还是在交换机之中。但又不是所有交换机都具有此功能,只有 VLAN

协议的第三层以上交换机才具有此功能，这一点通过查看相应交换机的说明书即可得知。

VTP 是一种在交换网络中共享相同 vlan 信息的协议。

STP 协议可以防止交换网络中出现广播风暴，并实现物理链路的备份。

1. VLAN 的基本配置

本节主要介绍 VLAN 的基本配置。

(1) VLAN 划分方式

VLAN 根据不同的需求，可以有多种划分方式，各种方式的优缺点比较如表 7-8 所示。

表 7-8 VLAN 划分方式

划 分 方 式	简单描述与优缺点比较	适 用 场 合
基于端口	按 VLAN 交换机上的物理端口和内部的 PVC（永久虚电路）端口来划分 优点：定义 VLAN 成员时非常简单，只要将所有的端口都定义为相应的 VLAN 组即可 缺点：如果某用户离开原来的端口到一个新的交换机的某个端口，需重新定义	适合于任何大小的网络
基于 MAC	这种划分 VLAN 的方法是根据每个用户主机的 MAC 地址来划分的 优点：当用户物理位置从一个交换机换到其他交换机时，VLAN 不用重新配置 缺点：初始化时，所有的用户都必须进行配置	适用于小型局域网
基于网络协议	VLAN 按网络层协议来划分，可分为 IP、IPX 等 VLAN 网络 优点：用户的物理位置改变了，不需要重新配置所属的 VLAN，而且可以根据协议类型来划分 VLAN，并且可以减少网络通信量，可使广播域跨越多个 VLAN 交换机 缺点：效率低下	适用于需要同时运行多协议的网络
基于 IP 组播	IP 组播即认为一个 IP 组播组就是一个 VLAN 优点：更大的灵活性，而且也很容易通过路由器进行扩展 缺点：适合局域网，主要是效率不高	适合于不在同一地理范围的局域网用户组成一个 VLAN
基于策略	基于策略的 VLAN 能实现多种分配，包括端口、MAC 地址、IP、协议等 优点：可根据自己的管理模式和需求来决定选择哪种类型的 VLAN 缺点：建设初期步骤烦琐	适用于需求比较复杂的环境
基于用户定义	是指为了适应特别的 VLAN 网络，根据具体的网络用户的特别要求来定义和设计 VLAN，而且可以让非 VLAN 群体用户访问 VLAN，但是需要提供用户密码，在得到 VLAN 管理的认证后才可以加入一个 VLAN	适用于安全性较高的环境

表 7-8 中，第一种划分方式又叫做静态划分，后面的几种划分方式统称为动态划分。静态划分安全、可靠，易于配置与维护；而动态划分高效、灵活，但缺乏安全保障。

(2) 静态 VLAN 配置

静态 VLAN 配置的过程如下所示。

① 准备工作：

vlan database # 进入 VLAN 配置模式

② 创建 VLAN：

vlan v_num name v_name # 创建命名 vlan（可以不要 name 命令）
no vlan v_num # 清除一个已存在的 VLAN

③ 将端口划入 VLAN：

switchport mode access # 配置接口接入模式


```
switchport access vlan 2 # 进入相应接口，让此接口归属 VLAN 2
```

④ 配置三层交换：

```
interface vlan 2
ip address 192.168.1.1 255.255.255.0 # 给 VLAN 2 配置 IP 地址与子网掩码
```

2. 中继协议

VLAN 中继协议（VLAN Trunking Protocol, VTP）通过网络保持 VLAN 配置统一性，管理增加、删除、调整的 VLAN，自动地将新的 VLAN 信息向网络中其他的交换机广播。此外，VTP 减少了那些可能导致安全问题的配置。

（1）相关概念

① VTP 模式：当交换机配置在 VTP Server 或透明的模式时，可以使用 CLI、控制台菜单、MIB 修改 VLAN 配置。

② VTP Domain：交换 VTP 更新信息的所有交换机必须配置为相同的管理域。

③ ISL（Inter-Switch Link）：是一个在交换机之间、交换机与路由器之间及交换机与服务器之间传递多个 VLAN 信息及 VLAN 数据流的协议，Cisco 交换机专用。

④ IEEE 802.1Q 标准：IEEE 制定的用于在中继链路上识别数据帧技术，它通过在帧头插入一个 VLAN 标识符来标识 VLAN，通常称为“帧标记”。

⑤ Trunk：在路由与交换领域，Trunk 是指 VLAN 的端口聚合，用来在不同的交换机之间进行连接，以保证在跨越多个交换机上建立的同一个 VLAN 的成员能够相互通信。

正如网络中也存在主机与服务器一样，应用 VTP 的交换机也分 3 种不同的工作模式。

① 服务器模式：它负责定义 VLAN 信息，并广播传输给其他交换机。

② 客户端模式：接收并使用来自服务器端发送过来的 VLAN 信息。配置命令如下。

```
switch# vlan database # 进入 VLAN 配置子模式
switch(vlan)# vtp client|server|transparent # 设置交换机工作模式
```

③ 透明模式：接收并转发来自服务器端发送过来的 VLAN 信息，但自己并不应用，是交换机的默认工作模式。

（2）VTP 配置

VTP 协议配置过程如表 7-9 所示。

表 7-9 VTP 协议配置过程

配置步骤	命令及命令注释	说明
①设置 VTP domain	<pre>vlan database # 进入 VLAN 配置模式 vtp domain vname # 设置 VTP 管理域名称 vname vtp server client # 设置交换机为服务器（或客户端）模式</pre>	VTP Domain 称为管理域，交换 VTP 更新信息的所有交换机必须配置为相同的管理域。核心交换机和分支交换机都要配置
②启用修剪功能	<pre>vlan pruning # 启用修剪功能</pre>	减少不必要的数据流量，充分利用带宽
③配置中继	<pre>interface fa0/1 switchport trunk encapsulation isl dot1q # 封装中继协议 switchport mode trunk # 端口设置为中继模式 switchport trunk allowed vlan vlan-list all</pre>	核心交换机以上都要配置，先进入交换机端口模式，再封装中继协议，配置端口中继模式。 vlan-list all 是允许所有或部分 VLAN 信息通过 Trunk 链路

(3) 生成树协议

生成树协议 (Spanning-Tree Protocol, STP), 主要功能是允许有多条交换或桥接的路径而不会对网络造成产生环路延时的影响。STP 主要配置命令如下。

① 整根路径成本

```
switch(config-if)# spanning-tree [vlan vlan-list] cost cost
```

② 整端口 ID

```
switch(config-if)# spanning-tree[vlan vlan-list] port-priority port-priority
```

端口权值默认为 128, 数字越小, 优先级越高。

③ 改 STP 时钟

```
switch(config)# spanning-tree [vlan vlan-list] hello-time seconds  
switch(config)# spanning-tree [vlan vlan-list] forward-time seconds  
switch(config)# spanning-tree [vlan vlan-list] max-age seconds
```

④ 端口上启用或禁用速端口

```
switch(config-if)# [no] spanning-tree portfast
```

⑤ 设备上启用或禁用速端口

```
switch(config)# [no]spanning-tree uplinkfast
```

7.4.2 一点一练

试题 1

虚拟局域网中继协议 (VTP) 有三种工作模式, 即服务器模式、客户机模式和透明模式, 以下关于这 3 种工作模式的叙述中, 不正确的是___(1)___。

- (1) A. 在服务器模式下可以设置 VLAN 信息
- B. 在服务器模式下可以广播 VLAN 信息
- C. 在客户机模式下不可以设置 VLAN 信息
- D. 在透明模式下不可以设置 VLAN 信息

试题 2

在下面关于 VLAN 的描述中, 不正确的是___(2)___。

- (2) A. VLAN 把交换机划分成多个逻辑上独立的交换机
- B. 主干链路 (Trunk) 可以提供多个 VLAN 之间通信的公共通道
- C. 由于包含了多个交换机, 所以 VLAN 扩大了冲突域
- D. 一个 VLAN 可以跨越多个交换机

试题 3

划分 VLAN 的方法有多种, 这些方法中不包括___(3)___。

- (3) A. 根据端口划分
- B. 根据路由由设备划分
- C. 根据 MAC 地址划分
- D. 根据 IP 地址划分

试题 4

下面有关 VLAN 的语句中, 正确的是___(4)___。

- (4) A. 虚拟局域网中继协议 VTP (VLAN Trunk Protocol) 用于在路由器之间交换不同 VLAN 的信息
- B. 为了抑制广播风暴, 不同的 VLAN 之间必须用网桥分隔
- C. 交换机的初始状态是工作在 VTP 服务器模式, 这样可以把配置信息广播给其他

交换机

- D. 一台计算机可以属于多个 VLAN，即它可以访问多个 VLAN，也可以被多个 VLAN 访问

试题 5

下面关于 802.1q 协议的说明中正确的是___(5)___。

- (5) A. 这个协议在原来的以太网帧中增加了 4 个字节的帧标记字段
B. 这个协议是 IETF 制定的
C. 这个协议在以太网帧的头部增加了 26 个字节的帧标记字段
D. 这个协议在帧尾部附加了 4 个字节的 CRC 校验码

试题 6

在生成树协议 STP 中，根交换机是根据___(6)___来选择的。

- (6) A. 最小的 MAC 地址
B. 最大的 MAC 地址
C. 最小的交换机 ID
D. 最大的交换机 ID

试题 7

下面的交换机命令中___(7)___命令为端口指定 VLAN。

- (7) A. S1(config-if)# vlan-membership static
B. S1(config-if)# vlan database
C. S1(config-if)# switchport mode access
D. S1(config-if)# switchport access vlan 1

试题 8

下面___(8)___设备可以转发不同 VLAN 之间的通信。

- (8) A. 二层交换机 B. 三层交换机 C. 网络集线器 D. 生成树网桥

试题 9

配置 VLAN 有多种方法，下面___(9)___命令不是配置 VLAN 的方法。

- (9) A. 把交换机端口指定给某个 VLAN
B. 把 MAC 地址指定给某个 VLAN
C. 由 DHCP 服务器动态地为计算机分配 VLAN
D. 根据上层协议来划分 VLAN

试题 10

下面是显示交换机端口状态的例子：

```
2950# show interface fastEthernet0/1 switchport
Name: fa0/1
Switchport: Enabled
Administrative mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: Disabled
Access Mode VLAN: 0 ((Inactive))
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Trunking VLANs Active: 1,2
Pruning VLANs Enabled: 2-1001
Priority for untagged frames: 0
Override vlan tag priority: FALSE
Voice VLAN: none
```

在以上显示的信息中, 端口 fa0/1 的链路模式被设置为____(10)____, 默认的 VLAN 为____(11)____。

- (10) A. 中继连接状态, 并要求对方也建立中继连接
B. 中继连接状态, 不要求与对方建立中继连接
C. 接入链路状态, 要求与对方建立中继连接
D. 接入链路状态, 不要求对方建立中继连接

- (11) A. VLAN0 B. VLAN1 C. VLAN2 D. VLAN3

7.4.3 解析与答案

试题 1 分析

VLAN 中继 (VLAN Trunk) 也称为 VLAN 主干, 是指在交换机与交换机或交换机与路由器之间连接情况下, 在互相连接的端口上配置中继模式, 使得属于不同 VLAN 的数据帧都可以通过这条中继链路进行传输。

VLAN 中继协议 (VLAN Trunk Protocol, VTP) 用于交换机设置 VLAN, 可以维护 VLAN 信息的一致性。VTP 有 3 种工作模式, 即服务器模式、客户模式和透明模式。服务器模式下可以设置 VLAN 信息, 服务器自动将这些信息广播到网上的其他交换机, 以便统一配置。在客户模式下, 交换机不能配置 VLAN 信息, 只能被动接受服务器的 VLAN 配置。在透明模式下是独立配置, 即可以配置 VLAN 信息, 但是不广播自己的 VLAN 信息, 同时它接收到服务器发来的 VLAN 信息后并不使用, 而是直接转发给别的交换机。

交换机的初始状态是工作在透明模式, 这种模式下有一个默认的 VLAN, 所有的端口都属于这个 VLAN。

试题 1 答案

- (1) D

试题 2 分析

此题主要考查了 VLAN 的基本知识。

VLAN 就是把物理上直接相连的网络划分为逻辑上独立的多个子网, 每个 VLAN 中包含有多个交换机, 所以 VLAN 可以把交换机划分为多个逻辑上独立的交换机。

VLAN 中继 (VLAN Trunk) 也称为 VLAN 主干, 是指交换机与交换机或者交换机与路由器之间连接时, 可以在相互的端口上配置中继模式, 使得属于不同 VLAN 的数据帧都可以通过这条中继线路进行传输, 所以主干链路可以提供多个 VLAN 之间的通信的公共通道。

每一个 VLAN 对应一个广播域, 处于不同 VLAN 上的主机不能进行通信, 不同 VLAN 之间的通信要通过路由器进行。所以 VLAN 并没有扩大冲突域。

试题 2 答案

- (2) C

试题 3 分析

VLAN 有以下几中常见的划分方法。

① 基于端口划分的 VLAN

这是最常应用的一种 VLAN, 目前绝大多数 VLAN 协议的交换机都提供这种 VLAN 配置方法。这种 VLAN 是根据以太网交换机的交换端口来划分的, 它是将 VLAN 交换机上的物理端口和 VLAN 交换机内部的 PVC (永久虚电路) 端口分成若干个组, 每个组构成一个虚拟网, 相当于一个独立的 VLAN 交换机。例如, 一个交换机的 1、2、3、4、5 端口被定义为虚拟网 A, 同一交换机的 6、7、8 端口组成虚拟网 B。这种方法的优点是定义 VLAN 成员时非常简单, 只要将所有的端口都定义为相应的 VLAN 组即可, 适合于任何大小的网络。

它的缺点是如果某用户离开了原来的端口,到了一个新的交换机的某个端口,必须重新定义。

② 基于 MAC 地址划分的 VLAN

这种 VLAN 是根据每个主机的 MAC 地址来划分,即对每个 MAC 地址的主机都配置其属于哪个组,VLAN 交换机跟踪属于 VLAN MAC 的地址。这种方式的 VLAN 允许网络用户从一个物理位置移动到另一个物理位置时,自动保留其所属 VLAN 的成员身份。

这种 VLAN 最大优点就是当用户物理位置移动时,即从一个交换机换到其他的交换机时,VLAN 不用重新配置,因为它是基于用户,而不是基于交换机的端口。这种方法的缺点是初始化时,所有的用户都必须进行配置,如果有几百个甚至上千个用户的话,配置是非常累的,所以这种划分方法通常适用于小型局域网。而且这种划分的方法也导致了交换机执行效率的降低,因为在每一个交换机的端口都可能存在很多个 VLAN 组的成员,保存了许多用户的 MAC 地址,查询起来相当不容易。另外,对于使用笔记本电脑的用户来说,他们的网卡可能经常更换,这样 VLAN 就必须经常配置。

③ 基于网络层协议划分的 VLAN

这种 VLAN 是根据每个主机的网络层地址或协议类型(如果支持多协议)划分的。VLAN 按网络层协议来划分,可分为 IP、IPX、DECnet、AppleTalk、Banyan 等 VLAN 网络。虽然这种划分方法是根据网络地址,比如 IP 地址,但它不是路由,与网络层的路由毫无关系。

这种方法的优点是用户的物理位置改变时,不需要重新配置所属的 VLAN,而且可以根据协议类型来划分 VLAN。另外,这种方法不需要附加的帧标签来识别 VLAN,这样可以减少网络的通信量。

这种方法的缺点是效率低,因为检查每一个数据包的网络层地址是需要消耗处理时间的(相对于前面两种方法),一般的交换机芯片都可以自动检查网络上数据包的以太网帧头,但要让芯片能检查 IP 帧头,需要更复杂的技术,同时也更费时。

④ 根据 IP 组播划分的 VLAN

IP 组播实际上也是一种 VLAN 的定义,即认为一个组播组就是一个 VLAN,这种划分的方法将 VLAN 扩大到了广域网,因此这种方法具有更大的灵活性,而且也很容易通过路由器进行扩展,当然这种方法不适合局域网,主要因为它的效率不高。

试题 3 答案

(3) B

试题 4 分析

用 VTP 设置和管理整个域内的 VLAN,在管理域内 VTP 自动发布配置信息,其范围包括所有 TRUNK 连接,如交换互连(ISL),802.10 和 ATM LAN (LANE)。当交换机加电时,它会周期性地送出 VTP 配置请求,直至接到近邻的配置(Summary)广播信息,从而进行结构配置必要的更新。

VTP 有 3 种工作模式,即服务器模式、客户模式和透明模式,其中服务器模式可以设置 VLAN 信息,服务器会自动将这些信息广播到网上其他交换机以统一配置;客户模式下交换机不能配置 VLAN 信息,只能被动接受服务器的 VLAN 配置,而透明模式下是独立配置。它可以配置 VLAN 信息,但是不广播自己的 VLAN 信息,同时它接收到服务器发来的 VLAN 信息后并不使用,而是直接转发给别的交换机。

交换机的初始状态是工作在服务器模式有一个默认的 VLAN,所有的端口都属于这个 VLAN 内。

为了抑制广播风暴,不同的 VLAN 之间必须用路由器分隔。一台计算机完全可以属于多个 VLAN。

试题 4 答案

(4) D

试题 5 分析

802.1q 协议由 IETF 制定, 根据 802.1q 封装协议, 发送数据包在原来的以太帧头部的源地址后面增加了一个 4 字节的 802.1q 标签, 之后接原来的以太网网的长度或者类型域。这 4 个字节的 802.1q 标签头包含两个字节的标签协议标识 (TPID), 值是 8100, 以及两个自己的标签控制信息 (TCI)。TPID 是 IEEE 定义的新的类型, 表明这是一个加了 802.1q 标签的文本。

试题 5 答案

(5) A

试题 6 分析

生成树协议 (Spanning Tree Protocol, STP) 是交换式以太网中的重要技术。其作用是在交换机之间存在的冗余链路的情况下能自动断开网络中的环路, 从而提高网络的可靠性和稳定性。其工作原理是通过交换机之间相互交换的网桥协议数据单元 BPDU, 使每个交换机了解交换网络中的拓扑结构信息。从而根据生成树算法维护交换网络中的树型结构, 避免环路出现。按照 802.1d 定义的生成树算法, 网络中的每台交换机 (网桥) 都有唯一的 6 字节 MAC 地址和 2 字节优先级值构成的网桥标识符, 又称为网桥 ID。每台交换机通过 BPDU 交换信息选举网桥 ID 最小值的网桥作为交换环中的根网桥。网络 ID 比较的顺序是先比较 2 字节的网桥优先级, 如果交换机的优先级都一样, 再比较其唯一的 MAC 地址, MAC 地址最小的交换机将成为根网桥。

试题 6 答案

(6) C

试题 7 分析

这 4 条命令解释如下。

```
switch (config-if) # vlan-membership static vlan_#
```

该命令为 Cisco I900 交换机端口分配 VLAN, 后面必须说明端口号。

```
switch (config-if) # vlan database
```

该命令用于 Cisco 2950 交换机, 从特权模式进入 VLAN 配置模式。

```
switch (config-if) # switchport mode access
```

该命令将端口设置为接入链路模式。

```
switch (config-if) # switchport access vlan 1
```

该命令用于 Cisco 2950 交换机, 把当前端口分配给 VLAN1。

试题 7 答案

(7) D

试题 8 分析

虚拟局域网 (Virtual Local Area Network, VLAN) 是根据管理功能、组织机构或应用类型对交换局域网进行分段而形成的逻辑网络, 其分段方法与设备的物理位置无关。虚拟局域网中的工作站可以不属于同一物理网段, 属于同一个 VLAN 的所有端口构成一个广播域, VLAN 之间的通信必须通过路由器或三层交换机进行转发。

试题 8 答案

(8) B

试题 9 分析

在交换机上实现 VLAN，可以采用静态或动态的方法。

静态分配 VLAN 为交换机的各个端口指定所属的 VLAN。这种基于端口的划分方法是把各个端口固定地分配给不同的 VLAN，任何连接到交换机的设备都属于接入端口所在的 VLAN。如果用户改变了接入端口而又想访问原来的 VLAN，则需要为该 VLAN 增加新的端口成员。

动态 VLAN 通过诸如 Cisco Works2000 之类的软件包来创建，可以根据设备的 MAC 地址、网络层协议、网络层地址、IP 广播域或管理策略来划分 VLAN。根据 MAC 地址划分 VLAN 的方法应用最多，一般交换机都支持这种方法。无论一台设备连接到交换网络的什么地方，接入交换机通过查询 VLAN 管理策略服务器（VLAN Management Policy Server，VMPS），根据设备的 MAC 地址就可以确定该设备的 VLAN 成员身份。这种方法使得用户可以在交换网络中改变接入位置，而仍能访问所属的 VLAN，但是当用户数量很多时，对每个用户设备分配 VLAN 的工作量是很大的管理负担。

基于网络层协议划分 VLAN 需要分析各种协议的地址格式并进行相应的转换，因此需要更多的处理开销。相比利用 MAC 地址划分 VLAN，这种方法在处理速度上不占优势。

试题 9 答案

(9) C

试题 10 分析

从以上信息的第 4 和第 5 行

```
Administrative mode: trunk  
Operational Mode: trunk
```

以及第 8 行

```
Negotiation of Trunking:Disabled
```

可知交换机端口处于中继连接状态，不要求与对方建立中继连接。从第 10 行

```
Trunking Native Mode VLAN: 1 (default)
```

可知默认的 VLAN 为 VLAN1。

试题 10 答案

(10) B

(11) B

7.5 考前冲刺

试题 1

IEEE 802.11 定义了无线局域网的两种工作模式，其中的____(1)____模式是一种点对点连接的网络，不需要无线接入点和有线网络的支持。

(1) A. Roaming

B. Ad Hoc

C. Infrastructure

D. DiffuseIR

试题 2

IEEE 802.11g 的物理层采用了扩频技术，工作在____(2)____频段。

(2) A. 600MHz

B. 800MHz

C. 2.4GHz

D. 19.2GHz

试题 3

IEEE 802 局域网中的地址分为两级，其中 LLC 地址是 (3) 。

- (3) A. 应用层地址
B. 上层协议实体的地址
C. 主机的地址
D. 网卡的地址

试题 4

快速以太网物理层规范 100BASE-TX 规定使用 (4) 。

- (4) A. 1 对 5 类 UTP, 支持 10M/100M 自动协商
B. 1 对 5 类 UTP, 不支持 10M/100M 自动协商
C. 2 对 5 类 UTP, 支持 10M/100M 自动协商
D. 2 对 5 类 UTP, 不支持 10M/100M 自动协商

试题 5

以太网的 CSMA/CD 协议采用坚持型监听算法。与其他监听算法相比,这种算法的主要特点是 (5) 。

- (5) A. 传输介质利用率低, 冲突概率也低 B. 传输介质利用率高, 冲突概率也高
C. 传输介质利用率低, 但冲突概率高 D. 传输介质利用率高, 但冲突概率低

试题 6

无线局域网标准 IEEE 802.11i 提出了新的 TKIP 协议来解决 (6) 中存在的安全隐患。

- (6) A. WAP 协议 B. WEP 协议 C. MD5 D. 无线路由器

试题 7

快速以太网标准比原来的以太网标准的数据速率提高了 10 倍，这时它的网络跨距（最大段长）（7）。

- (7) A. 没有改变 B. 变长了
C. 缩短了 D. 可以根据需要设定

试题 8

采用以太网链路聚合技术将 (8) 。

- (8) A. 多个逻辑链路组成一个物理链路 B. 多个逻辑链路组成一个逻辑链路
C. 多个物理链路组成一个物理链路 D. 多个物理链路组成一个逻辑链路

试题 9

以下属于万兆以太网物理层标准的是 (9) 。

- (9) A. IEEE 802.3u B. IEEE 802.3a C. IEEE 802.3e D. IEEE 802.3ae

试题 10

在生成树协议 STP 中，以下 (10) 命令用以配置接入层交换机的速端口。

- (10) A. switchport mode access B. switchport access vlan *vlan-id*
C. spanning-tree uplinkfast D. spanning-tree portfast

试题 11

当启用 VTP 修剪功能后, 如果交换端口中加入一个新的 VLAN, 则立即 (11) 。

- (11) A. 剪断与周边交换机的连接
B. 把新的 VLAN 中的数据发送给周边交换机
C. 向周边交换机发送 VTP 连接报文
D. 要求周边交换机建立同样的 VLAN

试题 12

IEEE 802.11i 标准增强了 WLAN 的安全性，下面关于 802.11i 的描述中，错误的是____(12)_____。

- (12) A. 加密算法采用高级数据加密标准 AES
- B. 加密算法采用对等保密协议 WEP
- C. 用 802.1x 实现了访问控制
- D. 使用 TKIP 协议实现了动态的加密过程

试题 13

关于无线局域网，下面叙述中正确的是____(13)_____。

- (13) A. 802.11a 和 802.11b 都可以在 2.4GHz 频段工作
- B. 802.11b 和 802.11g 都可以在 2.4GHz 频段工作
- C. 802.11a 和 802.11b 都可以在 5GHz 频段工作
- D. 802.11b 和 802.11g 都可以在 5GHz 频段工作

试题 14

以下关于 IEEE 802.3ae 标准的描述中，错误的是____(14)_____。

- (14) A. 支持 802.3 标准中定义的最小和最大帧长
- B. 支持 IEEE 802.3ad 链路汇聚协议
- C. 使用 1310nm 单模光纤作为传输介质，最大段长可达 10 公里
- D. 使用 850nm 多模光纤作为传输介质，最大段长可达 10 公里

试题 15

关于 IEEE 802.3 的 CSMA/CD 协议，下面结论中错误的是____(15)_____。

- (15) A. CSMA/CD 是一种解决访问冲突的协议
- B. CSMA/CD 协议适用于所有 802.3 以太网
- C. 在网络负载较小时，CSMA/CD 协议的通信效率很高
- D. 这种网络协议适合传输非实时数据

试题 16

交换机命令 SwitchA(VLAN)#vtp pruning 的作用是____(16)_____。

- (16) A. 退出 VLAN 配置模式
- B. 删除一个 VLAN
- C. 进入配置子模式
- D. 启动路由修剪功能

试题 17

利用交换机可以把网络划分成多个虚拟局域网 (VLAN)。一般情况下，交换机默认的 VLAN 是____(17)_____。

- (17) A. VLAN 0
- B. VLAN 1
- C. VLAN 10
- D. VLAN 1024

试题 18

通过交换机连接的一组工作站____(18)_____。

- (18) A. 组成一个冲突域，但不是一个广播域
- B. 组成一个广播域，但不是一个冲突域
- C. 既是一个冲突域，又是一个广播域
- D. 既不是冲突域，也不是广播域

试题 19

在 IEEE 802.11 标准中使用了扩频通信技术，下面选项中有关扩频通信技术说法正确的

是 (19)。

- (19) A. 扩频通信技术是一种带宽很宽的红外线通信技术
B. 扩频通信技术就是用伪随机序列对代表数据的模拟信号进行调制
C. 扩频通信系统的带宽随着数据速率的提高而不断扩大
D. 扩频通信技术就是扩大了频率许可证的使用范围

试题 20

新交换机出厂时的默认配置是 (21)。

- (20) A. 预配置为 VLAN 1, VTP 模式为服务器
B. 预配置为 VLAN 1, VTP 模式为客户机
C. 预配置为 VLAN 0, VTP 模式为服务器
D. 预配置为 VLAN 0, VTP 模式为客户机

试题 21

VLAN 中继协议 (VTP) 用于在大型交换网络中简化 VLAN 的管理。按照 VTP 协议, 交换机的运行模式分为 3 种: 服务器、客户机和透明模式。下面关于 VTP 协议的描述中, 错误的是 (21)。

- (21) A. 交换机在服务器模式下能创建、添加、删除和修改 VLAN 配置
B. 一个管理域中只能有一个服务器
C. 在透明模式下可以进行 VLAN 配置, 但不能向其他交换机传播配置信息
D. 交换机在客户机模式下不允许创建、修改或删除 VLAN

试题 22

EIA/TIA-568 标准规定, 在综合布线时, 如果信息插座到网卡之间使用无屏蔽双绞线, 布线距离最大为 (22) m。

- (22) A. 10 B. 30 C. 50 D. 100

试题 23

建筑物综合布线系统中的工作区子系统是指 (23)。

- (23) A. 由终端到信息插座之间的连线系统 B. 楼层接线间的配线架和线缆系统
C. 各楼层设备之间的互联系统 D. 连接各个建筑物的通信系统

试题 24

IEEE 802.11 采用了类似于 802.3 CSMA/CD 协议的 CSMA/CA 协议, 之所以不采用 CSMA/CD 协议的原因是 (24)。

- (24) A. CSMA/CA 协议的效率更高 B. CSMA/CD 协议的开销更大
C. 为了解决隐蔽终端问题 D. 为了引进其他业务

试题 25

IEEE 802.1q 协议的作用是 (25)。

- (25) A. 生成树协议 B. 以太网流量控制
C. 生成 VLAN 标记 D. 基于端口的认证

试题 26

千兆以太网标准 802.3z 定义了一种帧突发方式 (frame bursting), 这种方式是指 (26)。

- (26) A. 一个站可以突然发送一个帧
B. 一个站可以不经过程序就启动发送过程
C. 一个站可以连续发送多个帧

D. 一个站可以随机地发送紧急数据

试题 27

IEEE 802.3 规定的最小帧长为 64 字节, 这个帧长是指 (27)。

- (27) A. 从前导字段到校验和的长度 B. 从目标地址到校验和的长度
C. 从帧起始符到校验和的长度 D. 数据字段的长度

试题 28

通过交换机连接的一组工作站 (28)。

- (28) A. 组成一个冲突域, 但不是一个广播域
B. 组成一个广播域, 但不是一个冲突域
C. 既是一个冲突域, 又是一个广播域
D. 既不是冲突域, 也不是广播域

试题 29

IEEE 802.16 工作组提出的无线接入系统空中接口标准是 (29)。

- (29) A. GPRS B. UMB C. LTE D. WiMAX

试题 30

在局域网标准中, 100Base-T 规定从收发器到集线器的距离不超过 (30) 米。

- (30) A. 100 B. 185 C. 300 D. 1000

7.6 习题解析

试题 1 分析

在 802.11 的标准提案中, 规定了两种工作模式, 分别是有接入点 (Access Point, AP, 访问点、基站) 模式 (基础设施网络) 和无访问点模式 (Ad Hoc 网络)。其结构如图 7-15 所示。

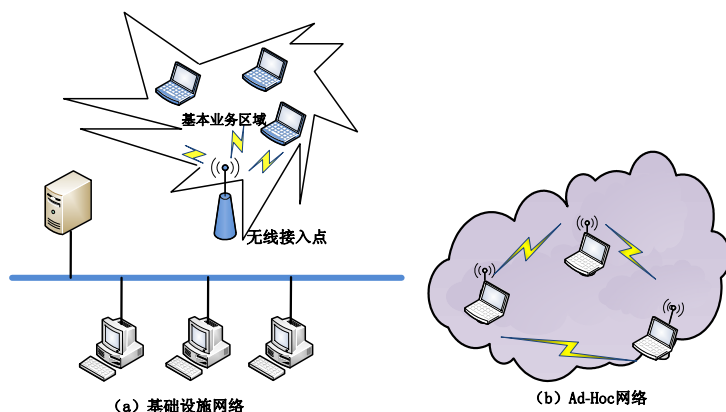


图 7-15 两种 WLAN 网络拓扑

在基础设施网络中, 无线终端通过接入点 (Access Point, AP) 访问骨干网设备, 或者互相访问。接入点如同一个网桥, 它负责在 802.11 和 802.3 MAC 协议之间进行转换。

Ad Hoc 网络是一种点对点连接, 不需要有线网络和接入点的支持, 以无线网卡连接的终端设备之间可以直接通信。这种拓扑结构适合在移动情况下快速部署网络, 主要用在军事领域, 也可以用在商业领域进行语音和数据传输。802.11 支持单跳的 Ad Hoc 网络, 当一个无线终端接入时首先寻找来自 AP 或其他终端的信标信号, 如果找到了信标, 则 AP 或其

他终端就宣布新的终端加入了网络；如果没有检测到信标，该终端就自行宣布存在于网络之中。

试题 1 答案

(1) B

试题 2 分析

IEEE 802.11 先后提出了以下多个标准,最早的 802.11 标准只能够达到 1~2Mb/s 的速度,在制定更高速度的标准时,就产生了 802.11a 和 802.11b 两个分支,后来又推出了 802.11g 的新标准,如表 7-10 所示。

表 7-10 无线局域网标准

标 准	运 行 频 段	主 要 技 术	数 据 速 率
802.11	2.4GHz 的 ISM 频段	扩频通信技术	1Mb/s 和 2Mb/s
802.11b	2.4GHz 的 ISM 频段	CCK 技术	11Mb/s
802.11a	5GHz U-NII 频段	OFDM 调制技术	54Mb/s
802.11g	2.4GHz 的 ISM 频段	OFDM 调制技术	54Mb/s

试题 2 答案

(2) C

试题 3 分析

由于局域网是分组广播式网络,网络层的路由功能是不需要的,所以在 IEEE 802 标准中,网络层简化成了上层协议的服务访问点 SAP。又由于局域网使用多种传输介质,而介质访问控制协议与具体的传输介质和拓扑结构有关,所以 IEEE 802 标准把数据链路层划分成了两个子层。与物理介质相关的部分叫做介质访问控制 MAC (Media Access Control) 子层,与物理介质无关的部分叫做逻辑链路控制 LLC (Logical Link Control) 子层。LLC 提供标准的 OSI 数据链路层服务,这使得任何高层协议(例如 TCP/IP, SNA 或有关的 OSI 标准)都可运行于局域网标准之上。局域网的物理层规定了传输介质及其接口的电气特性、机械特性、接口电路的功能以及信令方式和信号速率等。可以说 LLC 提供了上层访问的 SAP。

试题 3 答案

(3) B

试题 4 分析

100BASE-TX 使用的是两对抗阻为 100 欧姆的 5 类非屏蔽双绞线(UTP)或者屏蔽双绞线(STP),最大传输距离是 100 米。其中一对用于发送数据,另一对用于接收数据。100BASE-TX 采用的是 4B/5B 编码方式,即把每 4 位数据用 5 位的编码组来表示,该编码方式的码元利用率= $\frac{4}{5} \times 100\% = 80\%$ 。然后将 4B/5B 编码成 NRZI 进行传输。

100BASE-TX 标准的出现对促进网络结构化布线技术的发展起到了关键的作用,支持 10M/100M 自动协商。

试题 4 答案

(4) C

试题 5 分析

以太网可以采用以下三种监听算法。

① 非坚持型监听算法: 当一个站准备好帧, 发送之前先监听信道。

- a. 若信道空闲, 立即发送, 否则转 b;
- b. 若信道忙, 则后退一个随机时间, 重复 a。

由于随机时延后退, 从而减少了冲突的概率; 然而, 可能出现的问题是因为后退而使信道闲置一段时间, 这使信道的利用率降低, 而且增加了发送时延。

② I-坚持型监听算法: 当一个站准备好帧, 发送之前先监听信道。

- a. 若信道空闲, 立即发送, 否则转 b;
- b. 若信道忙, 继续监听, 直到信道空闲后立即发送。

这种算法的优缺点与前一种正好相反, 有利于抢占信道, 减少信道空闲时间; 但是多个站同时都在监听信道时必然发生冲突。

③ P-坚持型监听算法。其基本算法是先监听信道, 若空闲, 则以概率 P 发送。若信道忙, 则继续监听。这种算法汲取了以上两种算法的优点, 有效平衡冲突与信道利用率, 但较为复杂。

以太网的 CSMA/CD 协议采用坚持型监听算法。根据以上分析可知, 答案 B 是正确的。

试题 5 答案

(5) B

试题 6 分析

IEEE 802.11i 在 2004 年 6 月成为正式标准, 作为 802.11 家族的一部分, 802.11i 为 802.11a、802.11b 和 802.11g 无线局域网提供了全新的安全技术。802.11i 定义了新的密钥交换协议 TKIP (Temporal Key Integrity Protocol) 和高级加密标准 AES (Advanced Encryption Standard)。TKIP 是对 WEP (Wired Equivalency Protocol) 协议的改进, 它提供了报文完整性检查, 每个数据包使用不同的混合密钥 (Per-packet Key Mixing), 每次建立连接时生成一个新的基本密钥 (Re-keying 3), 这些手段的采用使得诸如密钥共享、碰撞攻击和重放攻击等无能为力, 从而弥补了 WEP 协议的安全隐患。

试题 6 答案

(6) B

试题 7 分析

与传统以太网一样, 快速以太网也要考虑冲突时槽 (slot) 和最小帧长 (L_{min}) 问题。快速以太网的数据速率提高了 10 倍, 而最小帧长没变, 所以冲突时槽缩小为 $5.12\mu s$ 。以太网的计算冲突时槽的公式为:

$$\text{slot} \approx 2S/0.7C + 2t_{phy}$$

其中 S 表示网络的跨距 (最长传输距离), $0.7C$ 为 0.7 倍光速 (信号传播速率), t_{phy} 是发送站物理层时延, 由于发送站发送和接收两次, 所以取其时延的两倍值。按照上式, 可得计算快速以太网跨距的计算公式:

$$S \approx 0.35C(L_{min}/R - 2t_{phy})$$

根据这个公式, 当 R 变大时, 网络跨距减小了。

试题 7 答案

(7) C

试题 8 分析

本题考查链路聚合技术。链路聚合是将两个或更多数据物理信道结合成一个单个的信道, 该信道以一个单个的更高带宽的逻辑链路出现。链路聚合一般用来连接一个或多个带宽需求大的设备, 例如连接骨干网络的服务器或服务器群。如果聚合的每个链路都遵循不同的

物理路径，则聚合链路也提供冗余和容错。通过聚合调制解调器链路或者数字线路，链路聚合可用于改善对公共网络的访问。链路聚合也可用于企业网络，以便在吉比特以太网交换机之间构建多吉比特的骨干链路。

试题 8 答案

(8) D

试题 9 分析

2002 年 6 月，IEEE 802.3ae 标准发布，支持 10Gb/s 的传输速率。传统以太网采用 CSMA/CD 协议，即带冲突检测的载波监听多路访问技术。与千兆以太网一样，万兆以太网基本应用于点到点线路，不再共享带宽，没有冲突检测，载波监听和多路访问技术也不再重要。千兆以太网和万兆以太网采用与传统以太网同样的帧结构，最大/最小帧长都不变。

试题 9 答案

(9) D

试题 10 分析

若接入层交换机配置了速端口，则速端口连接的 PC 一旦出现故障，需要更换另一台 PC 时，其端口状态立即由侦听状态转变成转发状态，中间省去了侦听到学习，学习到转发状态的转变过程，共节约了 30 秒的转发延迟时间。速端口一般配置在接入层交换机上，需要进入到交换的端口模式，其配置命令是 `(switch-if)#spanning-tree portfast`。

A 答案是调整交换机端口为接入模式，B 答案是让端口隶属于某个 vlan，C 答案是配置交换机的上行速链路。

试题 10 答案

(10) D

试题 11 分析

VLAN 中继协议 (VLAN Trunking Protocol, VTP) 用于在交换网络中简化 VLAN 的管理域。VTP 协议在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTR 报文可以传播到管理域中的所有交换机。

在默认情况下，所有交换机通过中继链路连接在一起，如果 VLAN 中的任何设备发出一个广播包、组播包或者一个未知的单播数据包，交换机都会将其洪泛 (flood) 到所有与源 VLAN 端口相关的各个输出端口上 (包括中继端口)。在很多情况下，这种洪泛转发是必要的，特别是在 VLAN 跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源 VLAN 的活动端口，则这种洪泛发送的数据包是无用的。

为了解决这个问题，可以使用静态或动态修剪的方法。所谓静态修剪，就是手工剪掉中继链路上不活动的 VLAN，在多个交换机组成多个 VLAN 的网络中，这种工作方式很容易出错，容易出现连接问题。

VTP 动态修剪允许交换机之间共享 VLAN 信息，也允许交换机从中继连接上动态地剪掉不活动的 VLAN，使得所有共享的 VLAN 都是活动的。例如，交换机 A 告诉交换机 B，它有两个活动的 VLAN 1 和 VLAN 2，而交换机 B 告诉交换机 A，它只有一个活动的 VLAN 1，于是，它们就共享这样的事实：VLAN 2 在它们之间的中继链路上是不活动的，应该从中继链路的配置中剪掉。这样做的好处是显而易见的，如果在交换机 B 上添加了 VLAN 2 的成员，交换机 B 就会通知交换机 A，它有了一个新的活动的 VLAN 2，于是，两个交换机动态地把 VLAN 2 添加到它们之间的中继链路配置中。

试题 11 答案

(11) C

试题 12 分析

IEEE 802.11 的 i 工作组致力于制定被称为 IEEE 802.11i 的新一代安全标准, 这种安全标准为了增强 WLAN 的数据加密和认证性能, 定义了 RSN (Robust Security Network) 的概念, 并且针对 WEP 加密机制的各种缺陷做了多方面的改进。

IEEE 802.11i 规定使用 802.1x 认证实现了访问控制和密钥管理方式, 在数据加密方面, 定义了 TKIP (Temporal Key Integrity Protocol)、CCMP (Counter-Mode/CBC-MAC Protocol) 和 WRAP (Wireless Robust Authenticated Protocol) 三种加密机制。其中 TKIP 采用 WEP 机制里的 RC4 作为核心加密算法, 可以通过在现有的设备上升级固件和驱动程序的方法达到提高 WLAN 安全的目的。CCMP 机制基于 AES (Advanced Encryption Standard) 加密算法和 CCM (Counter-Mode/CBC-MAC) 认证方式, 使得 WLAN 的安全程度大大提高, 是实现 RSN 的强制性要求。由于 AES 对硬件要求比较高, 因此 CCMP 无法通过在现有设备的基础上进行升级实现。WRAP 机制基于 AES 加密算法和 OCB (Offset Codebook), 是一种可选的加密机制。

试题 12 答案

(12) B

试题 13 分析

无线局域网标准的制定始于 1987 年, 当初是在 802.4L 组作为令牌总线的一部分来研究的, 其主要目的是用作工厂设备的通信和控制设施。1990 年, IEEE 802.11 小组正式独立出来, 专门从事制定 WLAN 的物理层和 MAC 层标准。1997 年颁布的 IEEE 802.11 标准运行在 2.4GHz 的 ISM (Industrial Scientific and Medical) 频段, 采用扩频通信技术, 支持 1Mb/s 和 2Mb/s 数据速率。随后又出现了两个新的标准, 1998 年推出的 IEEE 802.11b 标准也是运行在 ISM 频段, 采用 CCK (Complementary Code Keying) 技术, 支持 11 Mb/s 的数据速率。1999 年推出的 IEEE 802.11a 标准运行在 U-NII (Unlicensed National Information Infrastructure) 频段, 采用 OFDM (Orthogonal Frequency Division Multiplexing) 调制技术, 支持最高达 54Mb/s 的数据速率。目前的 WLAN 标准主要有 4 种, 如表 7-11 所示。

试题 13 答案

(13) B

试题 14 分析

IEEE 802.3ae 万兆以太网技术标准的物理层只支持光纤作为传输介质, 但提供了两种物理连接。一种是与传统以太网进行连接的、速率为 10Gb/s 的 LAN 物理层设备, 即 LAN PHY, 另一种是与 SDH/SONET 进行连接的速率为 9.58464Gb/s 的 WAN 物理层设备, 即 WAN PHY。通过引入 WAN PHY, 万兆以太网的帧可以与 SONETOC-192 帧结构融合, 从而能够通过 SONET 城域网提供端到端的以太网连接。

表 7-11 无线局域网标准

标 准	运 行 频 段	主 要 技 术	数 据 速 率
802.11	2.4GHz 的 ISM 频段	扩频通信技术	1Mb/s 和 2Mb/s
802.11b	2.4GHz 的 ISM 频段	CCK 技术	11Mb/s
802.11a	5GHz U-NII 频段	OFDM 调制技术	54Mb/s
802.11g	2.4GHz 的 ISM 频段	OFDM 调制技术	54Mb/s

每种物理连接都可使用 10GBASE-S（850nm 短波）、10GBASE-L（1310nm 长波）和 10GBASE-E（1550nm 长波）这三种规格的传输介质，最大传输距离分别为 300m、10000m 和 40000m。

在物理拓扑上，万兆以太网既支持星状连接（或扩展星状连接），也支持点到点连接，以及星状连接与点到点连接的组合。在万兆以太网的 MAC 子层，已不再采用 CSMA/CD 机制，只支持全双工传输方式。另外，万兆以太网还继承了 802.3 以太网的帧格式和最大/最小帧长度，从而能充分兼容已有的以太网技术，进而降低了对现有以太网进行万兆位升级的成本。

试题 14 答案

(14) D

试题 15 分析

CSMA/CD 是一种分解访问冲突的协议，应用在竞争发送的网络环境中，适合于传送非实时数据。在网络负载较小时，发送的速度很快，通信效率很高。在网络负载很大时，由于经常出现访问冲突，通信的效率很快就下降了。在千兆以太网中，当采用半双工传输方式时，要使用 CSMA/CD 协议来解决信道的争用问题。千兆以太网的全双工方式适用于交换机到交换机，或者交换机到工作站之间的点对点连接，两点间可同时进行发送与接收，不存在共享信道的争用问题，所以不需要采用 CSMA/CD 协议。2002 年 6 月发布的万兆以太网 802.3ae 10GE 标准只支持全双工方式，不支持单工和半双工，也不采用 CSMA/CD 协议。

试题 15 答案

(15) B

试题 16 分析

交换机命令 SwitchA(VLAN)#vtp pruning 的作用是启用路由修剪功能。在默认情况下，所有交换机通过中继链路连接在一起，如果 VLAN 中的任何设备发出一个广播包、组播包或者一个未知的单播数据包，交换机都会将其洪泛（flood）到所有与源 VLAN 端口相关的各个输出端口上（包括中继端口）。在很多情况下，这种洪泛转发是必要的，特别是在 VLAN 跨越多个交换机的情况下。然而，如果相邻的交换机上不存在源 VLAN 的活动端口，则这种洪泛发送的数据包是无用的。

为了解决这个问题，可以使用静态或动态的修剪方法。所谓静态修剪，就是手工剪掉中继链路上不活动的 VLAN。但是，手工修剪会遇到一些问题，主要是必须根据网络拓扑结构的改变经常重新配置中继链路。在多个交换机组成多个 VLAN 的网络中，这种工作方式很容易出错。

VTP 动态修剪允许交换机之间共享 VLAN 信息，也允许交换机从中继连接上动态地剪掉不活动的 VLAN，使得所有共享的 VLAN 都是活动的。例如，交换机 A 告诉交换机 B，它有两个活动的 VLAN 1 和 VLAN 2，而交换机 B 告诉交换机 A，它只有一个活动的 VLAN 1，于是，它们就共享这样的事实：VLAN 2 在它们之间的中继链路上是不活动的，应该从中继链路的配置中剪掉。

这样做的好处是显而易见的，如果以后在交换机 B 上添加了 VLAN 2 的成员，交换机 B 就会通知交换机 A，它有了一个新的活动的 VLAN 2，于是，两个交换机就会动态地把 VLAN 2 添加到它们之间的中继链路配置中。

试题 16 答案

(16) D

试题 17 分析

一般情况下，交换机默认的 VLAN-ID 是 VLAN1。交换机连接的所有工作站同属于 VLAN1。

试题 17 答案

(17) B

试题 18 分析

通过交换机连接的一组工作站同属于一个子网，是一个广播域。交换机的各个端口是不冲突的，这正是交换机优于集线器的特点。事实上，交换机的每个端口组成一个冲突域。

试题 18 答案

(18) B

试题 19 分析

扩展频谱通信技术起源于军事通信网络，其主要想法是将信号散布到更宽的带宽上以减少发生阻塞和干扰的机会。早期的扩频方式是频率跳动扩展频谱（Frequency Hopping Spread Spectrum, FHSS），更新的版本是直接序列扩展频谱（Direct Sequence Spread Spectrum, DSSS）。

图 7-16 表示了各种扩展频谱系统的共同特点。输入数据首先进入信道编码器，产生一个接近某中央频谱的较窄带宽的模拟信号。再用一个伪随机序列对这个信号进行调制。调制的结果是大大拓宽了信号的带宽，即扩展了频谱。在接收端，使用同样的伪随机序列来恢复原来的信号，最后再进入信道解码器来恢复数据。

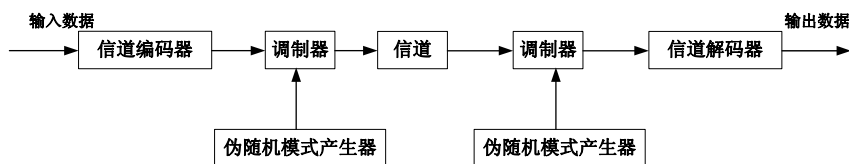


图 7-16 扩展频谱通信系统模型

伪随机序列由一个使用初值（称为种子 seed）的算法产生。算法是确定的，因此产生的数字序列并不是统计随机的。但如果算法设计得好，得到的序列就能够通过各种随机性测试，这就是被叫做伪随机序列的原因。重要的是，除非你知道算法与种子，否则预测序列是不可能的。因此，只有与发送器共享同一伪随机序列的接收器才能成功地对信号进行解码。

试题 19 答案

(19) B

试题 20 分析

新交换机出厂时的预配置为 VLAN 1，VIP 模式为服务器。

试题 20 答案

(20) A

试题 21 分析

VLAN 中继协议（VLAN Trunking Protocol, VTP）是 Cisco 公司的专利协议，用于在大型交换网络中简化 VLAN 的管理。VTP 协议在交换网络中建立了多个管理域，同一管理域中的所有交换机共享 VLAN 信息。一台交换机只能参加一个管理域，不同管理域中的交换机不共享 VLAN 信息。通过 VTP 协议，可以在一台交换机上配置所有的 VLAN，配置信息通过 VTP 报文可以传播到管理域中的所有交换机。

按照 VTP 协议，交换机的运行模式分为如下 3 种。

① 服务器模式（Server）。交换机在此模式下能创建、添加、删除和修改 VLAN 配置，并从中继端口发出 VTP 组播帧，把配置信息分发到整个管理域中的所有交换机。一个管理域中可以有多台服务器。

② 客户机模式（Client）。交换机在此模式下不允许创建、修改或删除 VLAN，但可以监听本管理域中其他交换机的 VTP 组播信息，并据此修改自己的 VLAN 配置。

③ 透明模式（Transparent）。交换机在此模式下可以进行 VLAN 配置，但配置信息不会传播到其他交换机。在透明模式下，可以接收和转发 VTP 帧，但是并不能据此更新自己的 VLAN 配置，只是起到通路的作用。

VTP 协议的优点有：

提供通过一个交换机在整个管理域中配置 VLAN 的方法；

提供跨不同介质类型（如 ATM、FDDI 和以太网）配置 VLAN 的方法；

提供跟踪和监视 VLAN 配置的方法；

保持 VLAN 配置的一致性。

试题 21 答案

(21) B

试题 22 分析

在进行结构化布线系统设计时，要考虑线缆长度的限制，表 7-12 是 EIA/TIA-568 标准提出的布线距离最大值。

表 7-12 综合布线系统各区域布线距离最大值

子 系 统	光 纤 (m)	屏蔽双绞线 (m)	非屏蔽双绞线 (m)
建筑群（楼栋间）	2000	800	700
主干（设备间到配线间）	2000	800	700
配线间到工作区信息插座		90	90
信息插座到网卡		10	10

试题 22 答案

(22) A

试题 23 分析

建筑物综合布线系统分为 6 个子系统：工作区子系统、水平布线子系统、干线子系统、设备间子系统、管理子系统和建筑群子系统，如图 7-17 所示。

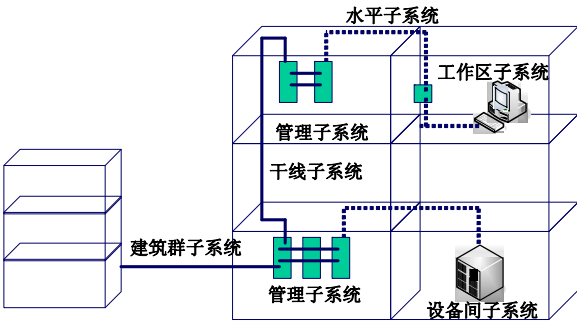


图 7-17 综合布线系统的组成

工作区子系统是由终端设备到信息插座的整个区域。一个独立的需要安装终端设备的区

域划分为一个工作区，工作区应支持电话、数据终端、计算机、电视机、监视器，以及传感器等多种终端设备。

各个楼层接线间的配线架到工作区信息插座之间所安装的线缆属于水平子系统。水平布线子系统的作用是将干线子系统线路延伸到用户工作区。

管理子系统设置在楼层的接线间内，由各种交连设备（双绞线跳线架、光纤跳线架）以及集线器和交换机等交换设备组成，交连方式取决于网络拓扑结构和工作区设备的要求。

干线子系统是建筑物的主干线缆，实现各楼层设备间子系统之间的互连。干线子系统通常由垂直的大对数铜缆或光缆组成，一头端接于设备间的主配线架上，另一头端接在楼层接线间的管理配线架上。

建筑物的设备间是网络管理人员值班的场所，设备间子系统由建筑物的进户线、交换设备、电话、计算机、适配器以及保安设施组成，实现中央主配线架与各种不同设备（如 PBX，网络设备和监控设备等）之间的连接。

建筑群子系统也称为园区子系统，它是连接各个建筑物的通信系统。

试题 23 答案

(23) A

试题 24 分析

CSMA/CA 类似于 802.3 的 CSMA/CD 协议，这种访问控制机制叫做载波监听多路访问/冲突避免协议。在无线网中进行冲突检测有时是困难的，例如两个站由于距离过大或者中间障碍物的分隔从而检测不到冲突，但是位于它们之间的第三个站可能会检测到冲突，这就是所谓隐蔽终端问题。采用冲突避免的办法可以解决隐蔽终端的问题。802.11 定义了一个帧间隔（Inter Frame Spacing, IFS）时间。另外还有一个后退计数器，它的初始值是随机设置的，递减计数直到 0。基本的操作过程是：

① 如果一个站有数据要发送并且监听到信道忙，则产生一个随机数设置自己的后退计数器并坚持监听。

② 听到信道空闲后等待 IFS 时间，然后开始计数。最先计数完的站可以开始发送。

③ 其他站在听到有新的站开始发送后暂停计数，在新的站发送完成后再等待一个 IFS 时间继续计数，直到计数完成开始发送。

分析这个算法发现，两次 IFS 之间的间隔是各个站竞争发送的时间。这个算法对参与竞争的站是公平的，基本上是按先来先服务的顺序获得发送的机会。

试题 24 答案

(24) C

试题 25 分析

在划分成 VLAN 的局域网中，每个数据包都被加上一个有关 VLAN 属性的帧标记，交换机之间根据帧标记来转发数据包。一个 VLAN 可以跨越多个交换机，带有 VLAN 标记的数据包在交换机之间的中继链路上传播，在进入 PC 时恢复原来的帧格式。

VLAN 帧标记有两种格式：一种是交换机间链路协议（Inter-Switch Link, ISL），这是 Cisco 公司的专利协议，适用于 Cisco 的 Catalyst 系列交换机；另一种是 IEEE 802.1q 协议。是在原来的以太帧中增加了 4 个字节的标记（Tag）字段，如下图所示，其中标记控制信息（Tag Control Information, TCI）包含 Priority、CFI 和 VID 三部分，各个字段的含义参见图 7-18。

802.1q 并没有定义优先级的含义，提供这种功能的是 802.1p 协议。另外，802.1p 协议还提供了组播过滤机制，以配合 IP 组播功能，使得 IP 组播流量不会被交换机广扩散。许多

高档交换机都把实现 802.1p 和 802.1q 作为重要的性能指标。

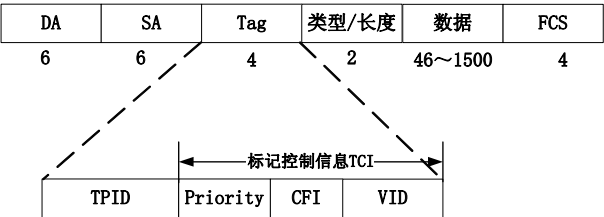


图 7-18 IEEE 802.1q 封装

试题 25 答案

(25) C

试题 26 分析

我们知道，在快速以太网中，时间槽是 512 位，在此期间内电波或光可以传输 400m 远，而在千兆以太网中，512 位的时间槽内电波或光的传输距离则只有 40m 远，这样的距离覆盖范围在实际应用中无法接受。因此千兆以太网采用帧突发的工作方式，具体过程是这样的：对于某站发送的第一个小于 512byte 的帧，依然使用载波扩展到 512byte，但随后发送的小于 512byte 的短帧不再使用载波扩展到 512byte，而是直接加入 96bit 的帧间隔序列后连续发送这些短帧，最长可以突发到 65536bit。因为在此网络中，如果某个站开始发送数据后，其他站都可以通过载波监听协议检测到其信号并抑制本站的数据发射。因此使用了帧突发的半双工千兆以太网的效率得到了较大的改善。

试题 26 答案

(26) C

试题 27 分析

本题考查以太网帧格式的基本概念。我们通常所指的以太网帧长是不包括前导字段的部分，也就是从目标地址开始到帧校验和结束的部分。同理以太网的最大帧长 1518 字节也是指这个范围。

试题 27 答案

(27) B

试题 28 分析

Cisco 公司的交换机的 VTP 模式有 3 种，分别是服务器模式(Server)、客户机模式(Client)和透明模式 (Transparent)。具体如表 7-13 所示。

表 7-13 VTP 三种模式比较

VTP 模 式	描 述
服务器模式 (Server)	提供 VTP 消息：包括 VLAN ID 和名字信息 学习相同域名的 VTP 消息 转发相同域名的 VTP 消息 可以添加、删除和更改 VLAN 信息，并写入 NVRAM
客户机模式 (Client)	请求 VTP 消息 学习相同域名的 VTP 消息 转发相同域名的 VTP 消息 不可以添加、删除和更改 VLAN 信息，不会写入 NVRAM

续表

VTP 模 式	描 述
透明模式 (Transparent)	不提供 VTP 消息 不学习 VTP 消息 转发 VTP 消息 可以添加、删除和更改 VLAN，但只在本地有效，在本地写入 NVRAM

新交换机出厂时的默认配置是预配置为 VLAN1，VTP 模式为服务器。

当交换机是在 VTP Server 或透明的模式，能在交换机配置 VLAN。当交换机配置在 VTP Server 或透明的模式，也可以修改 VLAN 配置。

当交换机在 VTP 的 Client 模式时，它会传送广播信息并从广播中学习新的信息。但是，不能直接在本机上增加、删除、修改 VLAN。也不能保持 VLAN 信息在非易失存储器中。当启动时，它会通过 Trunk 网络端口接收广播信息，学习配置信息。

当交换机在 VTP 透明的模式时，交换不会广播或从网络学习 VLAN 配置。但是可以在本机上修改、增加、删除 VLAN。

试题 28 答案

(28) C

试题 29 分析

WiMAX 即全球微波互联接入，也叫 802.16 无线城域网。WiMAX 是一项新兴的宽带无线接入技术，能提供面向互联网的高速连接，数据传输距离最远可达 50km。WiMAX 还具有 QoS 保障、传输速率高、业务丰富多样等优点。

试题 29 答案

(29) D

试题 30 分析

100Base-T 是一种以 100Mb/s 速率工作的局域网 (LAN) 标准，它通常被称为快速以太网标准，并使用 UTP (非屏蔽双绞线) 铜质电缆。规定从收发器到集线器的距离不超过 100 米。

试题 30 答案

(30) A

广域网和接入网技术

广域网（Wide Area Network, WAN）也称远程网。通常跨接很大的物理范围，所覆盖的范围从几十公里到几千公里，它能连接多个城市或国家，或横跨几个洲并能提供远距离通信，形成国际性的远程网络。

接入网是指骨干网络到用户终端之间的所有设备。其长度一般为几百米到几公里，因而被形象地称为“最后一公里”。

8.1 考点脉络

根据考试大纲，本章要求考生掌握以下几个方面的内容。

（1）广域网：包括 ATM、帧中继、ISDN、SONET/SDH 等广域网。

（2）接入网：包含 FTTx、xDSL、HFC 等接入网技术。

从历年的考试试题来看，本章的考点在综合知识考试中的平均分数为 1.1 分，约为总分的 1.4%。考试试题分数主要集中在 ISDN、FTTx、xDSL 这 3 个知识点上。

8.2 广域网

在广域网这个考点中，主要涉及 ATM、帧中继、ISDN、SONET/SDH 这 4 方面的内容。

8.2.1 考点精讲

异步传输模式（Asynchronous Transfer Mode, ATM）是实现 B-ISDN 业务的核心技术之一。

帧中继网络是一种用于统计复用分组交换数据通信的接口协议，分组长度可变，传输速度为 2.408Mb/s 或更高，没有流量控制也没有纠错。路由器是最重要的网络互联设备，其基本功能是子网划分、路由等。

综合业务数字网（ISDN），俗称“一线通”。它除了可以用来打电话，还可以提供诸如可视电话、数据通信、会议电视等多种业务，从而将电话、传真、数据、图像等多种业务综合在一个统一的数字网络中进行传输和处理。

SONET/SDH 定义了一组在光纤上传输光信号的速率和格式，通常统称为光同步数字传输网，是宽带综合数字网 B-ISDN 的基础之一，是对沿袭应用的准同步数字系列（Plesiochronous Digital Hierarchy, PDH）的一次革命。

1. 异步传输模式

本知识点包括信元及信元交换的基础概念、虚电路技术、信元头、AAL 适配层和 AAL 高层、ATM 的拥塞控制、ATM 的协议单元、子层、复用方式、信元速度和 ATM 适配层、

ATM 的虚通道和虚信道知识、ATM 信元交换基础知识。

(1) 同步传输和异步传输

电路交换网络都是按照时分多路复用的原理将信息从一个节点送到另一个节点的。根据工作模式的不同，可以分为两种。

① 同步传输模式 STM: 根据要求的数据速率，将一个逻辑信道分配为 1 个以上的时槽，在连接存在期时，时槽是固定分配的，即采用的是同步时分复用模式。

② 异步传输模式 ATM: 采用了与前面的不同方法分配时槽，它把用户数据组成为 53byte 的信元，信元随机到达，中间可以有间隙，信元准备好就可以进入信道，即采用的是统计时分复用模式。

在 ATM 中，信元不仅是传输的基本单位，也是交换的信息单位，它是虚电路式分组交换的一个特例。与分组相比，由于信元是固定长度的，因此可以高速地进行处理和交换。ATM 的典型数据速率为 150Mb/s, ATM 是面向连接的，所以在高速交换时要尽量减少信元的丢失。

(2) ATM 的分层体系结构

在 B-ISDN 中，建立了如表 8-1 所示的 4 层体系结构，总结了它们的功能以及与 OSI 层次的对应关系。

表 8-1 ATM 层次结构

层 次	子 层	功 能	与 OSI 对 应
ATM 高层		对用户数据的控制	高层
ATM 适配层	汇聚子层 (CS)	为高层数据提供统一接口	第四层
	拆装子层 (SAR)	分割和合并用户数据	
ATM 层		虚通道和虚信道的管理 信元头的组装和拆分 信元的多路复用 流量控制	第三层
ATM 物理层	传输汇聚子层 (TC)	信元校验和速率控制 数据帧的组装和分拆	第二层
	物理介质子层 (PMD)	比特定时 物理网络接入	第一层

① ATM 物理层

a. 物理介质子层 (PMD): 规定了传输介质、信号电平、比特定时等。不过 ATM 并未提供相应的规则，而是列出了一些可用的传输标准。例如，基于 5 类双绞线或光纤可达到 155.52Mb/s、622.08Mb/s、2488.32Mb/s (SONET 标准); 在 T3 信道上可达到 44.736Mb/s, 在 FDDI 上达到 100Mb/s。

b. 传输聚合子层: 提供了与 ATM 层的统一接口，该层完成类似数据链路层的功能。

② ATM 层

ATM 层相当于网络层的功能，它通过虚电路技术提供面向连接的服务。在 ATM 中，虚电路有两级，分别是虚通路 (VP) 和虚信道 (VC)。虚信道与 X.25 的虚电路相当，而虚通路则是由多条虚信道捆绑在一起形成的。由于 ATM 通常是在光纤的基础上建立的，因此不提供应答，它将少量的错误交给高层处理；另外，ATM 的目的是实现实时通信，因此对于偶然的信元错误是不重传的，对于要重传的通信由高层处理。

53 字节的 ATM 信元，是由 5 个字节的信元头和 48 个字节的数据组成的。在信元头中，有一些比较重要的字段需要掌握。

a. 虚通路标识符 (VPI)：8 位或 12 位，常用是 8 位，因此一个主机上的虚通路数通常是 256 个。

b. 虚信道标识符 (VCI)：16 位，因此理论上一个虚通路可以包含 65536 个虚信道，不过部分信道是用于控制的，并不传送用户数据。

c. 8 位头校验和：只对信元头进行校验，采用的是 X^8+X^2+X+1 的 8 位 CRC 校验。

d. 信元丢失优先级 (CLP)：在网络发生拥塞时提供指导，置为 1 的信元可抛弃。

e. 流控标志 (GFC)：用于主机和网络之间的流控或优先级控制。

f. 负载类型 (PTI)：区分不同的拥塞信息。

另外，有一个小知识点：在 ATM 逻辑通道中，是使用 VPI+VCI 的组合来标识连接的，在做 VP 交换或交叉连接时，只需要交换 VP，无须改变 VCI 的值。

③ ATM 适配层

ATM 适配层 (AAL) 负责处理高层来的信息，发送方把高层来的数字切成 48 字节长的 ATM 负载，接收方把 ATM 信元的有效负载重新组装成用户数据包。AAL 支持 4 种业务，有 5 种 AAL 层协议分别满足这些业务，如表 8-2 所示。

表 8-2 AAL 5 种协议

服 务 类 型	A 类	B 类	C 类	D 类
端到端定时	要求		不要求	
比特率	恒定	可变		
连接模式	面向连接			无连接
适配层协议	AAL1	AAL2	AAL3/4 和 AAL5	

a. AAL1：检测丢失和误插入信元，提供固定速率。

b. AAL2：用于传输面向连接的实时数据流，无错误检测，只检查顺序。

c. AAL3/4：原来是两个不同协议，分别对于 C 和 D，后来合并为一个，用于面向连接和无连接服务。

d. AAL5：它是实现 C、D 两类服务的新协议，它能够应用于 ATM 局域网访问。它采用 32 位 CRC 校验。

④ ATM 高层

ATM 高层主要规定了 4 类 5 种业务类型，以满足不同的 ATM 客户需求，如表 8-3 所示。

表 8-3 AAL 业务类型

业 务 类 型	特 点	适 用 应 用
CBR (固定比特率业务)	没有错误检查、流控和其他处理	交互式语音和视频流
RT-VBR (实时性变化比特率业务)	能够对信元的延迟和延迟变化进行控制	交互式压缩视频信号
NRT-VBR (非实时性变化比特率业务)	能够满足按时提交的需求	多媒体电子邮件
ABR (有效比特率业务)		突发式通信
UBR (不定比特率业务)	发生拥塞，信元可丢弃	IP 分组传送

2. 帧中继 (FR)

本知识点重点在于掌握帧中继的特点 (特别是工作层次、独有的拥塞控制, 以及在流量与差错控制方面的特点), 理解帧协议与结构, 特别是 FECN、BECN 这样有特色的帧字段。

帧中继协议在二层实现, 没有专门定义物理层接口 (可以使用 X.21、V.35、G.703、G.704 等接口协议), 在帧中继之上, 可以承载 IP 数据报, 而且其他协议甚至远程网桥协议都可以在帧中继上透明传输。帧中继协议是在第二层建立虚拟电路, 它用帧方式来承载数据业务, 因此第三层就被简化了, 而且它比 HDLC 要简单, 只做检错、不重传、没有滑动窗口式的流控, 只有拥塞控制, 把复杂的检错丢给高层去处理了。它所采用的接口协议体系如图 8-1 所示。

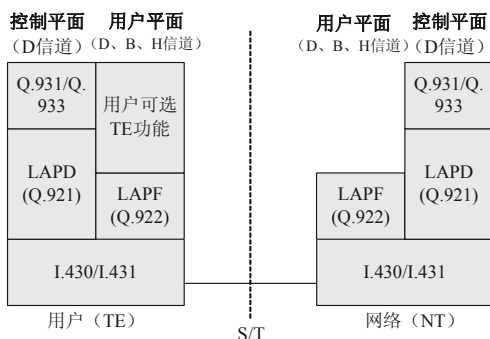


图 8-1 帧中继接口协议体系结构

帧中继使用的最核心协议是公共信道 D 进行信令传输控制协议 (Link Access Procedure on the D channel, LAPD), 它比 LAPB 更简单, 省去了控制字段。在其帧结构中有一些较有特色的地方和一些需要了解的知识如下。

① 信息字段: 就是用户要传送的信息, 长度是可变的, 默认长度为 1600。

② 帧中继采用了显式拥塞控制机制, 在帧头中有 FECN (向前拥塞比特)、BECN (向后拥塞比特) 两个特殊字段。如果 FECN 被设置为 1, 则说明帧在传送方向上出现了拥塞, 该帧到达接收端后, 接收方可对数据速率做相应的调整; 如果 BECN 被设置为 1, 则说明在与传送方向相反的方向上出现了拥塞, 该帧到达发送端后, 发送端可对数据速率做相应的调整。

③ 帧中继中包括一个 DE (优先丢弃比特), 如果设置为 1, 当网络拥塞时会优先丢弃。

④ 与 X.25 相类似, 帧中继也使用虚拟电路的方式提供面向连接的服务, 在帧头中包括一个 DLCI (数据链路连接标识符) 字段, 每个 DLCI 都标识出了一个虚电路, 其中 DLCI0 是用于信令传输的。

帧中继支持交换虚电路 (SVC) 和固定虚电路 (PVC, 永久虚电路) 两种虚电路技术。

a. 交换虚电路: 控制交换虚电路的信息是在信令信道 (DLCI=0) 上传送的。这些消息采用的是 LAPF 协议 (LAPF 的帧格式与 LAPD 基本相同, 但没有 FECN、BECN 和 DE 字段)。

b. 固定虚电路: 帧中继协议在早期并没有建立交换虚电路的信令, 只能够通过网络管理建立永久虚电路。PVC 的管理协议控制端到端的连接, 是通过带外信令的无编号信息帧传送的。

而基于这两种不同的虚电路技术, 帧中继就可以向用户提供不同的服务质量, 这些服务

质量参数如表 8-4 所示。

表 8-4 服务质量参数

服 务 质 量	缩 写	含 义
接入速度	AR	指 DTE 可获得的最大速率
约定突发量	Bc	指在测定时间内允许发送的数据量, $Bc = CIR \times \text{时间}$
超突发量	Be	指在测定时间内超出 Bc 部分的数据量→尽力传送。 $Be = EIR \times \text{时间}$
约定数据速率	CIR	正常状态下的数据速率
扩展的数据速率	EIR	指允许用户增加的数据速率

使用帧中继进行远程联网的主要优点是：透明传输，面向连接，帧长可变，速率高，能应对突发数据传输、没有流控和重传，开销小。但它并不适于对延迟敏感的应用（音频和视频），无法保证可靠的提交。

3. 综合业务数据网

本知识点的主要内容就是与 ISDN 相关的各种知识，包括 B 信道、D 信道、H 信道、BRI、PRI 等。

ISDN（综合业务数据网）可以分为窄带 ISDN（N-ISDN）和宽带 ISDN（B-ISDN）两种。其中 N-ISDN 是将数据、声音、视频信号集成进一根数字电话线路的技术。它的服务由两种信道构成：一是传送数据的运载信道（又称为 B 信道，每个信道 64Kb/s）；二是用于处理管理信号及调用控制的信令信道（又称为 D 信道，每个信道 16Kb/s 或 64Kb/s）。然后将这两类信道进行组成，形成两种不同的 ISDN 服务，分别是基速率接口（ISDN BRI）和主速率接口（ISDN PRI）。

（1）基速率接口：一般由 2B+D 组成，常用于小型办公室与家庭，用户可以用 1B 做数据通信，另 1B 保留为语音通信，但无法使用 D 通道。当然如果需要，也可以同时使用 2B 通道（128Kb/s）做数据通信。

（2）主速率接口：PRI 包括两种，一是美标的 23B+1D（64Kb/s 的 D 信道），达到与 T1 相同的 1.533Mb/s 的 DS1 速度；二是欧标的 30B+2D（64Kb/s 信道），达到与 E1 相同的 2.048Mb/s 的速度。另外，电话公司通常可以将若干个 B 信道组合成不同的 H 信道。

N-ISDN 定义了物理层、数据链路层和网络层的部分功能。在物理层建立了一个 64Kb/s 的线路交换连接，还提供了网络终端适配器的物理接口；在数据链路层则使用了 LAPD 来管理所有的控制和信令功能；其网络层处理所有的线路交换及分组交换服务。

B-ISDN 的关键技术是异步传输模式（ATM），采用 5 类双绞线或光纤，数据速率可达 155Mb/s，可以传输无压缩的高清晰度电视信号（HTV）。

4. SONET/SDH

本知识点主要在于理解 SONET/SDH 的工作原理、优缺点、适用性。

同步光纤网络（SONET）和同步数字层级（SDH），是一组有关光纤信道上的同步数据传输的标准协议，常用于物理层构架和同步机制。SONET 是由美国国家标准化组织（ANSI）颁布的美国标准版本，SDH 是由国际电信同盟（ITU）颁布的国际标准版本。两者均为传输网络物理层技术，传输速率可高达 10Gb/s，除了使用的复用机制有所不同，而其余技术均相似。SDH 的网络元素主要有同步光纤线路系统、终端复用器（TM）、分插复用器（ADM）和同步数字交叉连接设备（DXC）。典型的 SDH 应用是在光纤上的双环应用。SDH 每秒传送 8K SDH 帧（STM-N），SDH 是提供字节同步的物理层介质。

IPoverSDH 是以 SDH 网络作为 IP 数据网络的物理传输网络，它使用链路适配及成帧协议对 IP 数据报进行封装，然后按字节同步的方式把封装后的 IP 数据报映射到 SDH 的同步净荷封装（SPE）中。目前广泛使用 PPP 对 IP 数据报进行封装，并采用 HDLC 的帧格式。PPP 提供多协议封装、差错控制和链路初始化控制等功能，而 HDLC 帧格式负责同步传输路上的 PPP 封装的 IP 数据帧的定界。

SONET/SDH 可以应用于 ATM 或非 ATM 环境。SONET/SDH（POS）上的数据报利用点对点协议（PPP），将 IP 数据报映射到 SONET 帧负载中。在 ATM 环境下，SONET/SDH 线路连接方式可能为多模式、单模式或 UTP。SONET 是基于传输在基本比特率是 51.840Mb/s 的多倍速率，或 STS-1 的。而 SDH 是基于 STM-1 的，数据传输速率为 155.52Mb/s，与 STS-3 相当。

目前常用的 SONET/SDH 数据传输速率如表 8-5 所示。

表 8-5 SONET/SDH 数据传输速率列表

SONET 信号	比特率/Mb/s	SDH 信号	SONET 性能	SDH 性能
STS-1 和 OC-1	51.840	STM-0	28 DS-1s 或 1 DS-3	21 E1s
STS-3 和 OC-3	155.520	STM-1	84 DS-1s 或 3 DS-3s	63 E1s 或 1 E4
STS-12 和 OC-12	622.080	STM-4	336 DS-1s 或 12 DS-3s	252 E1s 或 4 E4s
STS-48 和 OC-48	2488.320	STM-16	1344 DS-1s 或 48 DS-3s	1008 E1s 或 16 E4s
STS-192 和 OC-192	9953.280	STM-64	5376 DS-1s 或 192 DS-3s	4032 E1s 或 64 E4s
STS-768 和 OC-768	39813.120	STM-256	21504 DS-1s 或 768 DS-3s	16128 E1s 或 256 E4s

8.2.2 一点一练

试题 1

以下关于帧中继网的叙述中，错误的是___（1）___。

- （1）A. 帧中继提供面向连接的网络服务
- B. 帧在传输过程中要进行流量控制
- C. 既可以按需提供带宽，也可以适应突发式业务
- D. 帧长可变，可以承载各种局域网的数据帧

试题 2

帧中继地址格式中表示虚电路标识符的是___（2）___。

- （2）A. CIR B. DLCI C. LMI D. VPI

试题 3

在 ATM 网络中，AAL5 用于 LAN 仿真，以下有关 AAL5 的描述中不正确的是___（3）___。

- （3）A. AAL5 提供面向连接的服务 B. AAL5 提供无连接的服务
- C. AAL5 提供可变比特率的服务 D. AAL5 提供固定比特率的服务

试题 4

利用 SDH 实现广域网互联，如果用户需要的数据传输速率较小，可以用准同步数字系列（PDH）兼容的传输方式在每个 STM-1 帧中封装___（4）___个 E1 信道。

- （4）A. 4 B. 63 C. 255 D. 1023

试题 5

下面关于帧中继网络的描述中，错误的是___（5）___。

- （5）A. 用户的数据速率可以在一定的范围内变化

- B. 既可以适应流式业务，又可以适应突发式业务
- C. 帧中继网可以提供永久虚电路和交换虚电路
- D. 帧中继虚电路建立在 HDLC 协议之上

8.2.3 解析与答案

试题 1 分析

帧中继通过 PVC 和 SVC 为用户提供通信服务，这是一种面向连接的服务。帧在传输过程中要通过流量整形技术来实现端速率的匹配，通过 BECN-N 后向显示阻塞通告、FECN-前向显示阻塞通告、CID-承诺传输率和 BC-数据平均传输率等参数来实现流量整形。因此可以实现按需提供带宽，也可以适用突发式的业务。在帧中继中其帧长度可变，最大帧长可以达到 1008 个字节。

试题 1 答案

(1) B

试题 2 分析

CIR: 承诺信息速率，按照协议应当达到的信息传输速率，也指与用户预先约定的数据速率。

DLCI: 数据链路连接标识符，在帧中继网络中表示 PVC（永久虚电路）或 SVC（交换式虚电路）的值。

LMI: 帧中继本地管理接口，是对基本的帧中继标准的扩展。它是路由器和帧中继交换机之间的信令标准，提供帧中继管理机制。其中提供了许多管理复杂互联网络的特性，包括全局寻址、虚电路状态消息和多路发送等。

VPI: ATM 的虚通道。

试题 2 答案

(2) B

试题 3 分析

AAL5 常用来支持面向连接的数据服务，用于面向连接的文件传输和数据网络应用程序，该程序中在数据传输前已预先设置好连接。这种服务提供可变比特率但不需要为传送过程提供有限延时。AAL5 也可以用来支持无连接的服务，该服务的例子包括数据报流量，通常也包括数据网络应用程序，在该程序中在数据传输前没有预先设置连接。但是 AAL5 并不能提供固定比特率的服务。因此 D 是错误的。

试题 3 答案

(3) D

试题 4 分析

本题考查 SDH 接入的基础知识。同步数字系列（Synchronous Digital Hierarchy, SDH）是一种将复接、线路传输及交换功能融为一体的物理传输网络。SDH 不是一种协议，也不是指一种传输介质，而是一种传输技术。SDH 网络主要使用光纤通信技术，但也可使用微波和卫星传送。SDH 可以对网络实现有效的管理、提供实时业务监控、动态网络维护、不同厂商设备间的互通等多项功能，能大大提高网络资源利用率、降低网络管理及维护的费用，是运营商主要的基础设施网络。

SDH 采用的信息结构等级称为同步传送模块 STM-N（N=1, 4, 16, 64 等），最基本的模块为 STM-1（155.520Mb/s），4 个 STM-1 同步复用构成 STM-4（622.080Mb/s），16 个 STM-1 同步复用构成 STM-16（2488.320Mb/s）。

如果用户需要的数据传输速率较小,则 SDH 还可以提供准同步数字系列(Plesiochronous Digital Hierarchy, PDH)兼容的传输方式。这种方式在 STM-1 中封装了 63 个 E1 信道,可以同时向 63 个用户提供 2Mb/s 的接入速率。PDH 兼容方式提供两种接口,一是传统的 E1 接口,例如路由器上的 G.703 转 V.35 接口,另一种是封装了多个 E1 信道的 CPOS (Channel POS) 接口,路由器通过一个 CPOS 接口接入 SDH 网络,并通过封装的多个 E1 信道连接多个远程站点。

试题 4 答案

(4) B

试题 5 分析

帧中继(FR)在第二层建立虚电路,用帧方式承载数据业务,因而第三层被简化掉了。在用户平面,FR 帧比 HDLC 帧操作简单,只检查错误,不再重传,没有滑动窗口式的流量控制机制,只有拥塞控制。

FR 的虚电路分为永久虚电路(Permanent Virtual Circuit, PVC)和交换虚电路(Switch Virtual Circuit, SVC)。PVC 是在两个端用户之间建立的固定逻辑连接,为用户提供约定的服务。帧中继交换设备根据预先配置的虚电路表把数据帧从一段链路交换到另外一段链路,最终传送到接收用户。SVC 是通过 ISDN 信令协议(Q931/Q933)临时建立的逻辑信道,它以呼叫的形式建立和释放连接。很多帧中继网络只提供 PVC 业务,不提供 SVC 业务。

帧中继网为用户提供约定信息速率(CIR)和扩展的信息速率(EIR),以及约定突发量(Bc)和超突发量(Be),这些参数之间有如下关系:

$$Bc = Tc \times CIR$$

$$Be = Tc \times EIR$$

其中, Tc 为数据速率测量时间。网络应该保证用户以等于或低于 CIR 的速率传送数据。对于超过 CIR 的 Bc 部分,在正常情况下能可靠地传送,但若出现网络拥塞,则会被优先丢弃。对于 Be 部分的数据,网络将尽量传送,但不保证传送成功。对于超过 Bc+Be 的部分,网络拒绝接收。这是在保证用户正常通信的前提下防止网络拥塞的主要手段,对各种数据通信业务有很强的适应能力。

在帧中继网中,用户的信息速率可以在一定的范围内变化,从而既可以适应流式业务,又可以适应突发式业务。

试题 5 答案

(5) D

8.3 接入网

在接入网这个考点中,主要涉及 FTTx、xDSL 和 HFC 这三方面的内容。

8.3.1 考点精讲

FTTx+LAN 技术是一种利用光纤加五类网络线方式实现宽带接入方案,实现千兆光纤到小区(大楼)中心交换机,中心交换机和楼道交换机以百兆光纤或五类网络线相连。

xDSL 是一种新的传输技术,在现有的铜质电话线路上采用较高的频率及相应调制技术,即利用在模拟线路中加入或获取更多的数字数据的信号处理技术来获得高传输速率(理论值可达到 52Mb/s)。

混合光纤同轴电缆网(Hybrid Fiber-Coaxial, HFC)是一种经济实用的综合数字服务宽带网接入技术。

1. FTTx+LAN 接入

本知识点在于了解 FTTx 技术，实现 FTTH 的 ATM-PDS 和 STM-PDS 技术，实现 FTTB 的 APON 和 EPON 技术，了解它们的关键特性与基本原理。

(1) FTTx 技术

所谓光纤通信 (FTTx)，是指利用光导纤维 (简称光纤) 传输光波信号的一种通信方法。相对于以电为媒介的通信方式而言，光纤通信的主要优点包括：传输频带宽，通信容量大；传输损耗小；抗电磁干扰能力强；线径细、重量轻；资源丰富等。

随着光纤通信技术的平民化，以及高速以太网的发展，现在许多宽带智能小区就是采用以千兆以太网技术为主干、充分利用光纤通信技术完成接入的。

实现高速以太网的宽带技术常用的方式是 FTTx+LAN，即光纤+局域网。根据光纤深入用户的程度，可以分为以下 5 种。

- ① FTTC (Fiber To The Curb)：光纤到路边。
- ② FTTZ (Fiber To The Zone)：光纤到小区。
- ③ FTTB (Fiber To The Building)：光纤到楼。
- ④ FTTF (Fiber To The Floor)：光纤到楼层。
- ⑤ FTTH (Fiber To The Home)：光纤到户。

(2) 无源光网技术

无源光网 (PON) 是实现 FTTB 的关键性技术。其在光分支点不需要节点设备，只需安装一个简单的光分支器即可，因此具有节省光缆资源、带宽资源共享、节省机房投资、设备安全性高、建网速度快、综合建网成本低等优点。目前无源光网技术主要有 APON 和 EPON 两种。

① APON：ATM-PON 基于 ATM 的无源光网络，分别选择 ATM 和 PON 作为网络协议和网络平台，其上/下行方向的信息传输都采用 ATM 传输方案，下行速率为 622Mb/s 或 155Mb/s，上行速率为 155Mb/s。光节点到前端的距离可达 10~20km，或者更长。采用无源双星型 (PDS) 拓扑，使用时分复用和时分多址技术，可以实现信元中继、局域网互联、电路仿真、普通电话业务等。

② EPON：Ethernet-PON，基于以太网的无源光网络，是以太网技术发展的新趋势，其下行速率为 1000Mb/s 或者 100Mb/s，上行速率为 100Mb/s。在 EPON 中，传送的是可变长度的数据报，最长可为 65535 个字节；而在 APON 中，传送的是 53 个字节的固定长度信元。它简化了网络结构，提高了网络速度。

2. 电话线路有 xDSL

本知识点在于了解各种电话接入技术的特点、速度和关键技术。利用普通电话线接入是成本最低、应用最广的接入技术，表 8-6 总结了各种常见技术。

表 8-6 多种接入技术比较

大 类	接 入 技 术	用 户 速 率	技 术 特 点	其 他
PSTN	拨号接入	300~54Kb/s	通过调制技术(ASK、FSK、PSK 及其结合)在模拟信道上进行数据通信	最常用的设备是 Modem，每次速度的提高都依赖于调制技术的发展

续表

大 类	接 入 技 术	用 户 速 率	技 术 特 点	其 他
ISDN	ISDN BRI 2B+D16	64~128Kb/s	使用 TDM 技术将可用的信道分成一定数量的固定大小时隙	能够实现按需拨号、按需分配带宽 (1B 数据、1B 语音; 或 2B 数据)
	ISDN PRI 23B+D64 30B+D64	1.544Mb/s 2.048Mb/s	使用 TDM (时分复用) 技术, 复用更多的信道, 适用于更大的数据通信	通常用于数字语音服务等, 也可以用于宽带需求的数据通信应用
xDSL	HDSL—— 高速数字用 户环路	1.544Mb/s 2.048Mb/s	对称 xDSL 技术, T1 使用 2 条线路 (使用 CAP 编码), E1 使用 3 条线路 (使用 2B1Q 编码), 3~5km	典型应用于 PBX 网络连接、蜂窝基站、数字环路载波系统、交互 POPs、互联网服务器、专用数据网
	SDSL	1.544Mb/s 2.048Mb/s	0.4mm 双绞线的最大传输距离是 3km 以上	它是 HDSL 的单线版本, 也称为“单线数据用户线”
	ADSL—— 非对称数字 用户环路	上行: 512Kb/s~1Mb/s; 下行: 1~8Mb/s	使用 FDM 和回波抵消技术实现频带分隔, 线路编码为 DMT 和 CAP	非对称的 xDSL 技术, 适用于 VOD、互联网接入、LAN 接入、多媒体接入等
	RADSL—— 速率自适应 用户数字线	上行: 640Kb/s~12Mb/s; 下行: 128Kb/s~1Mb/s	支持同步和非同步传输, 支持数据和语音同时传输, 可根据双绞线的质量优劣和距离动态调整	适用于质量千差万别的农村、山区等地区, 且不怕下雨、高温等反常天气
	VDSL	可在较短的距离上获得极高的速率。当传输距离为 300~1000m 时, 下行速率可达 52Mb/s, 上行速度可达 1.5~2.3Mb/s, 而当传输距离在 1.5km 以上时, 下行速率就降到 13Mb/s, 上行速率能够维持在 1.6~2.3Mb/s 左右		

注: (1) ADSL 现在比较成熟的标准包括两种, 即全速率 ADSL 标准 G.DMT (上行速率为 1.5Mb/s, 下行速率为 8Mb/s, 要求用户安装 POTS 分离器, 复杂且价格昂贵, 适用于小型办公室); G.Lite (上行速率为 512Kb/s, 下行速率为 1.5Mb/s, 省去复杂的 POTS 分离器, 成本较低且易于安装, 适用于普通家庭)。

(2) ADSL 现在提供了固定接入和 VLAN 接入两种方式。

3. HFC 接入

本知识点在于了解同轴电缆接入的网络基本结构、关键设备 (Cable Modem)、编码技术、复用技术以及传输速率。

HFC 是将光缆敷设到小区, 然后通过光电转换节点, 利用有线电视 CATV 的总线式同轴电缆连接到用户, 提供综合电信业务的技术。这种方式可以充分利用 CATV 原有的网络, 建网快、造价低, 逐渐成为最佳的接入方式之一。HFC 是由光纤干线网和同轴电缆分配网通过光节点站结合而成的, 一般光纤干线网采用星型拓扑, 同轴电缆分配网采用树型结构。

在同轴电缆的技术方案中, 用户端需要使用一个称为 Cable Modem (电缆调制解调器) 的设备, 它不单纯是一个调制解调器, 还集成了调谐器、加/解密设备、桥接器、网络接口卡、虚拟专网代理和以太网集线器的功能于一身, 它无须拨号, 可提供随时在线的永远连接。其上行速率已达 10Mb/s 以上, 下行速率更高。

其采用的复用技术是 FDM (频分复用技术), 使用的编码格式是 64QAM 调制。HFC 网络拓扑结构如图 8-2 所示。

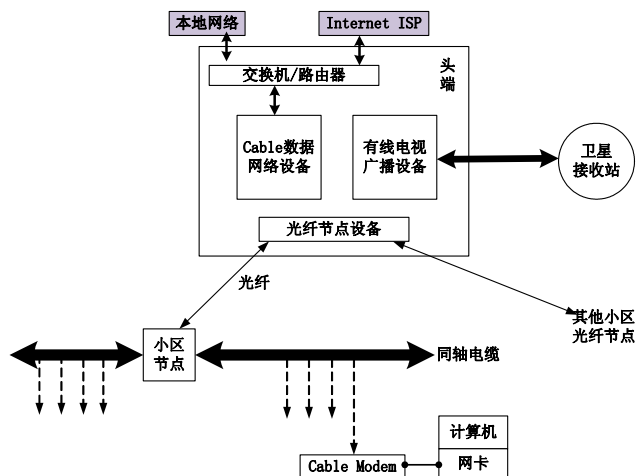


图 8-2 HFC 有线电视网络接入图

8.3.2 一点一练

试题 1

在各种 xDSL 技术中，能提供上/下行信道非对称传输的是____(1)____。

- (1) A. ADSL 和 HDSL B. ADSL 和 VDSL
C. SDSL 和 VDSL D. SDSL 和 HDSL

试题 2

通过 CATV 电缆访问因特网，在用户端必须安装的设备是____(2)____。

- (2) A. ADSL Modem B. Cable Modem
C. 无线路由器 D. 以太网交换机

试题 3

通过 ADSL 访问 Internet，在用户端通过____(3)____和 ADSL Modem 连接 PC。

- (3) A. 分离器 B. 电话交换机
C. DSLAM D. IP 路由器

试题 4

数字用户线（DSL）是基于普通电话线的宽带接入技术，可以在铜质双绞线上同时传送数据和话音信号。下列选项中，数据速率最高的 DSL 标准是____(4)____。

- (4) A. ADSL B. VDSL
C. HDSL D. RADSL

试题 5

接入 Internet 的方式有多种，下面关于各种接入方式的描述中不正确的是____(5)____。

- (5) A. 以终端方式入网，不需要 IP 地址
B. 通过 PPP 拨号方式接入，需要有固定的 IP 地址
C. 通过代理服务器接入多台主机可以共享一个 IP 地址
D. 通过局域网接入可以有固定的 IP 地址，也可以有动态分配的 IP 地址

8.3.3 解析与答案

试题 1 分析

xDSL 技术就是用数字技术对现有的模拟用户线进行改造，使它能够承担宽带业务。虽

然标准模拟电话信号的频带被限制在 300~3400kHz 的范围内，但用户线本身实际通过的信号频率仍然超过 1MHz，因此 xDSL 技术把 0~4000kHz 的低端频谱都留给传统电话使用，把原来没有使用的高端频谱留给用户上网使用。DSL 就是用户数字线的缩写，而 x 则表示数字用户线上实现不同的宽带方案。

SDSL：单线对数字用户线路，对称模式。

HDSL：高数据速率数字用户线路，对称模式。

VDSL：甚高数据速率数字用户线路，非对称模式。

非对称数字用户线路（Asymmetrical Digital Subscriber Loop，ADSL）其特点就是上行速度和下行速度不一样，并且往往是下行速度大于上行速度。从 1989 年以来，ADSL 走过了一个漫长的历程。下行速率从 1.5Mb/s 提高到 8Mb/s（当然这是以缩短传输距离为代价的），上行速率也已经提高到 640Kb/s。ADSL 的服务端设备和用户端设备之间通过普通的电话铜线连接，无须对入户线缆进行改造就可以为现有的大量电话用户提供 ADSL 宽带接入。随着标准和技术的成熟及成本的不断降低，ADSL 日益受到电信运营商和用户的欢迎，成为接入 Internet 的主要方式之一。

试题 1 答案

(1) B

试题 2 分析

在 CATV 的技术方案中，用户端需要使用一个称为 Cable Modem（电缆调制解调器）的设备，它不单纯是一个调制解调器，还集成了调谐器、加/解密设备、桥接器、网络接口卡、虚拟专网代理和以太网集线器的功能于一身，它无须拨号、可提供随时在线的永远连接。其上行速度已达 10Mb/s 以上，下行速率更高。

试题 2 答案

(2) B

试题 3 分析

本题考查 ADSL 接入知识。ADSL 接入方式分为虚拟拨号和准专线两种。采用虚拟拨号的用户需要安装 PPPoE（PPP over Ethernet）或 PPPoA（PPP over ATM）客户端软件，以及类似于 Modem 的拨号程序，输入用户名称和用户密码即可连接到宽带接入站点。采用准专线方式的用户使用电信部门静态或动态分配的 IP 地址，开机即可接入 Internet。其拓扑图如图 8-3 所示。

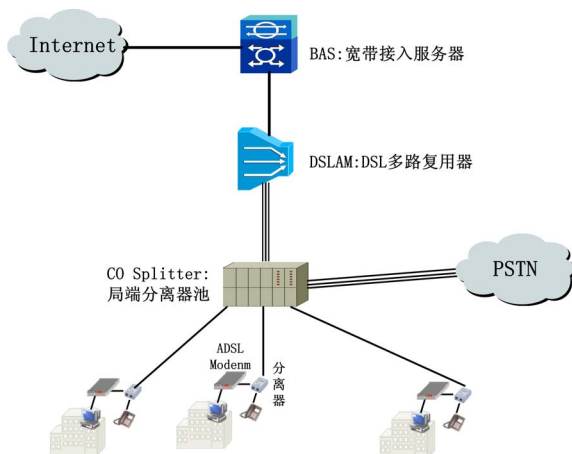


图 8-3 ADSL 宽带接入图

上图表示家庭个人应用的连接线路，PC 通过 ADSL Modem→分离器→入户接线盒→电话线→DSL 接入复用器（DSL Access Multiplexer, DSLAM）连接 ATM 或 IP 网络，而语音线路通过分离器→入户接线盒→电话线→DSL 接入复用器接入电话交换机。

试题 3 答案

(3) A

试题 4 分析

各种常见的 xDSL 接入技术如下。

① HDSL（高速数字用户线路）

HDSL 是最常见也是最成熟的 DSL 业务。它以 1.544Mb/s 的 T1 数据速率在长达 3.6 公里（12000 英尺）的线路上对称传送数据。一般来说，HDSL 是一种 T1 业务，它不需要中继器，但确实使用两个线路。语音电话业务不能在一线路上使用。它不是设计用于家庭用户，而是用于电话公司自己的馈电线路、局间连接、因特网业务和专用数据网络。

② SDSL（对称数字用户线路）

SDSL 是一种对称的双向 DSL 业务，它基本上与 HDSL 相同，但是在一个双绞线线路上使用。它可以提供高达 1.544Mb/s T1 速率的数据速率。SDSL 是速率自适应技术，和 HDSL 一样，SDSL 也不能同模拟电话共用线路。

③ ADSL（非对称数字用户线路）

ADSL 是一种非对称技术，意思是下行数据速率高于上行数据速率。正如所提到的一样，这种技术适用于这样的典型因特网会话，即其中从 Web 服务器下载的信息多于上载的信息。ADSL 在高于语音业务频率范围的频率范围中使用，因此同一线路可承载模拟话音和数字数据传输。上行速率范围为 16K/s 到高达 768K/s。

④ VDSL（甚高速数字用户线路）

VDSL 就是 ADSL 的快速版本。使用 VDSL，短距离内的最大下传速率可达 55Mb/s，上传速率可达 19.2Mb/s，甚至更高（不同厂家的芯片组，支持的速度不同。同一厂家的芯片组，使用的频段不同，提供的速度也不同）。

⑤ RADSL

速率自适应数字用户线路（Rate-Adaptive DSL，RADSL）是在 ADSL 基础上发展起来的新一代接入技术，这种技术允许服务提供者调整 xDSL 连接的带宽以适应实际需要并且解决线长和质量问题，为远程用户提供可靠的数据网络接入手段。它的特点是：利用一对双绞线传输；支持同步和非同步传输方式；速率自适应，下行速率从 1.5Mb/s 到 8Mb/s，上行速率从 16Kb/s 到 640Kb/s；支持同时传数据和语音。

试题 4 答案

(4) B

试题 5 分析

本题是考查考生对用户接入 Internet 的常见方式的了解，由于终端仅仅共享同一台主机的信息，所以不需要单独的 IP 地址。通过代理服务器接入方式可以多台主机共享代理服务器的 IP 地址。通过局域网方式接入可以获得固定的 IP 地址，也可以是动态分配的方式。这个问题其实可以从平时设置网卡的 IP 地址的界面看到，可以自动获取，也可以手工指定 IP 地址。使用 PPP 拨号方式也可以使用动态分配方式获取 IP，如常见的通过电话线拨号等，所以答案是 B。

试题 5 答案

(5) B

8.4 考前冲刺

试题 1

N-ISDN 有两种接口, 即基本速率接口 (2B+D) 和基群速率接口 (30B+2D), 有关这两种接口的描述中正确的是___(1)___。

- (1) A. 基群速率接口中, B 信道的带宽为 16Kb/s, 用户发送用户信息
B. 基群速率接口中, D 信道的带宽为 16Kb/s, 用户发送信令信息
C. 基本速率接口中, B 信道的带宽为 64Kb/s, 用户发送用户信息
D. 基本速率接口中, D 信道的带宽为 64Kb/s, 用户发送信令信息

试题 2

ADSL 是一种宽带接入技术, 这种技术使用的传输介质是___(2)___。

- (2) A. 电话线
B. CATV 电缆
C. 基带同轴电缆
D. 无线通信网

试题 3

在光纤通信标准中, OC-3 的数据速率是___(3)___。

- (3) A. 51Mb/s
B. 155Mb/s
C. 622Mb/s
D. 2488Mb/s

试题 4

使用 ADSL 拨号上网, 需要在用户端安装___(5)___协议。

- (4) A. PPP
B. SLIP
C. PPTP
D. PPPoE

试题 5

按照美国制定的光纤通信标准 SONET, OC-48 的线路速率是___(5)___Mb/s。

- (5) A. 41.84
B. 622.08
C. 2488.32
D. 9953.28

试题 6

以下属于对称数字用户线路 (Symmetrical Digital Subscriber Line) 的是___(6)___。

- (6) A. HDSL
B. ADSL
C. RADSL
D. VDSL

试题 7

在 HFC 网络中, Cable Modem 的作用是___(7)___。

- (7) A. 用于调制解调和拨号上网
B. 用于调制解调以及作为以太网接口
C. 用于连接电话线和用户终端计算机
D. 连接 ISDN 接口和用户终端计算机

试题 8

ADSL 采用的两种接入方式是___(8)___。

- (8) A. 虚拟拨号接入和专线接入
B. 虚拟拨号接入和虚电路接入
C. 虚电路接入和专线接入
D. 拨号虚电路接入和专线接入

试题 9

FTTx+LAN 接入网采用的传输介质为___(9)___。

- (9) A. 同轴电缆
B. 光纤
C. 5 类双绞线
D. 光纤和 5 类双绞线

试题 10

ATM 适配层的功能是____(10)_____。

- (10) A. 分割和合并用户数据
B. 信元头的组装和拆分
C. 比特定
D. 信元校验

8.5 习题解析

试题 1 分析

本题考查 N-ISDN 两种接口的特征。

N-ISDN 采用两种标准的用户/网络接口,即基本速率接口(BRI)和基群速率接口(PRI)。

基本速率接口: 2B+D, 其中 B 为 64Kb/s 的数字信道, D 为 16Kb/s 的数字信道。

基群速率接口: 也称为“一次群速率接口”, 即 30B+2D, B 和 D 都是 64Kb/s 的数字信道。B 信道主要用于用户传送用户信息流。D 信道主要用于传送电路交换信令信息, 也用于传送分组交换的数据信息。

试题 1 答案

(1) C

试题 2 分析

ADSL 是一种宽带接入技术。所谓宽带, 可以从两方面理解。首先是它提供的带宽比较高, 下载速率可以达到 8Mb/s, 甚至更高, 上传速率也可以达到 644Kb/s~1 Mb/s。其次是它采用频分多路技术在普通电话线划分出上行、下行和话音等不同的信道, 从而实现上网和通话同时传输。

试题 2 答案

(2) A

试题 3 分析

本题考查常用数字传输系统的基础知识。1985 年, Bellcore 提出同步光纤网传输标准 SONET (Synchronous Optical Network)。1989 年, CCITT 参照 SONET 制定了同步数字系列标准 SDH (Synchronous Digital Hierarchy), 两者有细微差别, 如表 8-7 所示。

表 8-7 SONET/SDH 数据传输速率列表

SONET 信号	比特率/Mb/s	SDH 信号	SONET 性能	SDH 性能
STS-1 和 OC-1	51.840	STM-0	28 DS-1s 或 1 DS-3	21 E1s
STS-3 和 OC-3	155.520	STM-1	84 DS-1s 或 3 DS-3s	63 E1s 或 1 E4
STS-12 和 OC-12	622.080	STM-4	336 DS-1s 或 12 DS-3s	252 E1s 或 4 E4s
STS-48 和 OC-48	2488.320	STM-16	1344 DS-1s 或 48 DS-3s	1008 E1s 或 16 E4s
STS-192 和 OC-192	9953.280	STM-64	5376 DS-1s 或 192 DS-3s	4032 E1s 或 64 E4s
STS-768 和 OC-768	39813.120	STM-256	21504 DS-1s 或 768 DS-3s	16128 E1s 或 256 E4s

SONET/SDH 是一种通用的传输体制, 不仅适于光纤, 也适于微波和卫星传输, 是宽带综合业务数字网(B-ISDN)的基础。SONET/SDH 采用 TDM 技术, 是对原来应用于骨干网的准同步数字系列(Plesiochronous Digital Hierarchy, PDH)的改进。SONET 用于北美地区和日本, SDH 用于中国和欧洲地区。

试题 3 答案

(3) B

试题 4 分析

数字用户线路 (Digital Subscriber Line, DSL) 是以铜质电话线为传输介质的通信技术。非对称 DSL (Asymmetric DSL, ADSL) 技术适用于对双向带宽要求不一样的应用, 如 Web 浏览、多媒体点播和信息发布等。ADSL 在一对铜线上支持上行速率 640Kb/s~1 Mb/s、下行速率 1Mb/s~8Mb/s, 有效传输距离在 3~5 千米范围以内, 支持上网冲浪, 同时还可以提供话音服务。

ADSL 接入方式分为虚拟拨号和准专线两种。采用虚拟拨号的用户需要安装 PPPoE (PPP Over Ethernet) 或 PPPoA (PPP Over ATM) 客户端软件, 以及类似于 Modem 的拨号程序, 输入用户名称和用户密码即可连接到宽带接入站点。采用准专线方式的用户使用电信部门静态或动态分配的 IP 地址, 开机即可接入 Internet。

试题 4 答案

(4) D

试题 5 分析

参考试题 3 解析中, 表 8-7 中的数据。得到 OC-48 的线路速率是 2488.32Mb/s。

试题 5 答案

(5) C

试题 6 分析

数字用户线路 (Digital Subscriber Line, DSL) 是基于普通电话线的宽带接入技术。它可以在一根铜线上分别传送数据和语音信号, 其中数据信号并不通过电话交换设备, 并且不需要拨号, 属于专线上网方式。DSL 有许多模式, 通常把所有的 DSL 技术统称为 xDSL, x 代表不同种类的 DSL 技术。

按数据传输的上、下行传输速率是否相同, DSL 可以分为对称和非对称两种传输模式。对称 DSL 技术中, 上、下行传输速率相同, 主要有 HDSL、SDSL 等, 用于替代传统的 TI/EI 接入技术。

高比特率用户数字线 HDSL 采用两对或三对双绞线提供全双工数据传输, 支持 $n \times 64\text{Kb/s}$ ($n=1, 2, 3, \dots$) 的各种速率, 较高的速率可达 1.544Mb/s 或 2.048Mb/s, 传输距离可达 3~5km, 技术上比较成熟, 在视频会议、远程教学和移动电话基站连接等方面得到了广泛应用。

SDSL (单线路用户数字线) 在单一双绞线上支持多种对称速率的连接, 用户可根据数据流量, 选择最经济合适的速率。在 0.4mm 双绞线上的最大传输距离可达 3km 以上, 能够支持诸如电视会议和协同计算等各种要求上、下行通信速率一致的应用。SDSL 标准目前还处于发展中。

非对称 DSL 技术的上、下行传输速率不同, 适用于对双向带宽要求不一样的应用, 例如 Web 浏览、多媒体点播、信息发布等。

ADSL (Asymmetrical Digital Subscriber Line) 是一种非对称 DSL 技术, 在一对铜线上可提供上行速率 512Kb/s~1Mb/s, 下行速率 1~8Mb/s, 有效传输距离在 3~5km。在进行数据传输的同时还可以使用第三个信道进行 4kHz 的语音传输。现在比较成熟的 ADSL 标准有 G.DMT 和 G.Lite 两种。G.DMT 是全速率的 ADSL 标准, 支持 8Mb/s 的下行速率及 1.5Mb/s 的上行速率, 但它要求用户端安装 POTS 分离器, 比较复杂且价格昂贵; G.Lite 标准速率较低, 下行速率为 1.5Mb/s, 上行速率为 512Kb/s, 但省去了 POTS 分离器, 成本较低且便于安装。G.DMT 较适用于小型办公室 (SOHO), 而 G.Lite 则更适用于普通家庭。

RADSL (速率自适应用户数字线) 支持同步和非同步传输方式, 下行速率为 640Kb/s~

12Mb/s，上行速率为 128Kb/s~1Mb/s，也支持数据和语音同时传输，具有速率自适应的特点。RADSL 可以根据双绞线的质量和传输距离动态调整用户的访问速度。RADSL 允许通信双方的 MODEM 寻找流量最小的频道来传送数据，以保证一定的数据传输速率。RADSL 特别适用于线路质量千差万别的农村、山区等地区使用。

VDSL（甚高比特率数字用户线）可在较短的距离上获得极高的传输速率，是各种 DSL 中速度最快的一种。在一对铜双绞线上，VDSL 的下行速率可以扩展到 52Mb/s，同时允许 1.5~2.3Mb/s 的上行速率，但传输距离只有 300~1000m。当下行速率降至 13Mb/s 时，传送距离可达到 1.5km 以上，此时上行速率为 1.6~2.3Mb/s 左右。传输距离的缩短，会使码间干扰大大减少，数字信号处理就大为简化，所以其设备成本要比 ADSL 低。

试题 6 答案

(6) A

试题 7 分析

电缆调制解调器（Cable Modem，CM）是基于 HFC 网络的宽带接入技术。CM 是用户设备与同轴电缆网络的接口。在下行方向，它接收前端设备（Cable Modem Termination System，CMTS）发送来的 QAM 信号，经解调后传送给 PC 的以太网接口。在上行方向，CM 把 PC 发送的以太网帧封装在时隙中，经 QPSK 调制后，通过上行数据通路传送给 CMTS。

CM 不单纯是调制解调器，它集 MODEM、调谐器、加/解密设备、桥接器、网络接口卡、SNMP 代理和以太网集线器等功能于一身，无须拨号上网，不占用电话线路，可永久连接。大多数 Cable Modem 提供一个标准的 10Base-T 以太网接口，可以同用户的 PC 或局域网集线器相连。

试题 7 答案

(7) B

试题 8 分析

ADSL 采用的两种接入方式是虚拟拨号接入和专线接入。虚拟拨号就是和普通 56K MODEM 拨号一样，通过 PPPoE 协议进行账号验证、IP 地址分配等过程建立连接，是面向家庭用户的接入方式。ADSL 专线接入是在用户安装好 ADSL MODEM 后，在 PC 中配置 IP 地址、子网掩码、默认网关等参数，开机后用户端和局端自动建立起一条链路。所以专线接入方式是有固定 IP 地址的接入方式，费用较高，多在大型网吧中使用。

试题 8 答案

(8) A

试题 9 分析

实现高速以太网宽带接入的常用方法是 FTTx+LAN，即光纤+局域网。这里 FTTx（Fiber To The x）是指：FTTZ（光纤到小区）、FTTB（光纤到楼）和 FTTH（光纤到家庭）。FTTx+LAN 采用千兆以太网交换技术，利用光纤+5 类双绞线来实现用户高速接入。它能够为用户提供双向 10Mb/s 或 100Mb/s 的标准以太网接口，并提供基于 IP 级数的各种服务。FTTx+LAN 用户接入方式如图 8-4 所示。

通过局域网以 10~100Mb/s 的速度接入宽带 IP 网络，小区内的交换机和局端交换机以光纤相连，小区内采用 5 类综合布线系统，网络可扩展性强、投资规模小。

试题 9 答案

(9) D

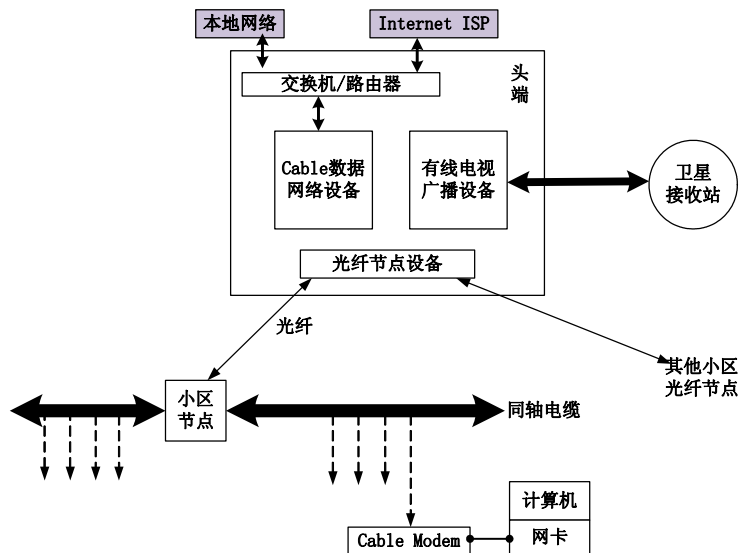


图 8-4 HFC 有线电视网络接入拓扑图

试题 10 分析

ATM 各个协议层的功能如表 8-8 所示。

表 8-8 ATM 层次结构

层 次	子 层	功 能	与 OSI 对 应
ATM 高层		对用户数据的控制	高层
ATM 适配层	汇聚子层 (CS)	为高层数据提供统一接口	第四层
	拆装子层 (SAR)	分割和合并用户数据	
ATM 层		虚通道和虚信道的管理 信元头的组装和拆分 信元的多路复用 流量控制	第三层
ATM 物理层	传输汇聚子层 (TC)	信元校验和速率控制 数据帧的组装和拆分	第二层
	物理介质子层 (PMD)	比特定时 物理网络接入	第一层

试题 10 答案

(10) A

因特网与网络互联技术

计算机网络最终目的是实现网络互联和数据通信。TCP/IP 协议栈是实现计算机网互联和数据通信的基础。基于 TCP/IP 协议栈，又会涉及 IP 寻址、子网规划、交换技术和路由选择技术等核心知识点。本章就是围绕这些知识点一一展开的。

9.1 考点脉络

因特网和互联网络技术是网络工程师考域中最为重要的一个考点，一般集中在软考网络工程师考试中的综合知识题部分。

根据考试大纲，要求考生掌握以下几个方面的内容。

- (1) IP 地址：包括 IPv4 地址分类、IPv4 地址寻址、VLSM、CIDR、IPv6。
- (2) 交换与路由：包含交换技术、路由协议及其配置、路由器基本配置、NAT、ACL。
- (3) 网络规划：包含规划原则、规划步骤。

从历年的考试试题来看，本章的考点在综合知识考试中的平均分数为 15 分，约为总分的 20%。考试试题分数主要集中在 IPv4 地址分类、VLSM、CIDR、IPv6、路由协议及其配置、NAT、ACL 和网络规划 8 个知识点上。

9.2 IP 地址

在 IP 地址这个考点中，主要涉及 IPv4 地址分类、VLSM、CIDR 和 IPv6 这 4 方面的内容。

9.2.1 考点精讲

IPv4 地址可以分为 A、B、C、D、E 五类，但真正用于节点通信的是 A、B、C 三类，D 类地址用于组播，E 类地址作为保留地址，用于科研。

VLSM 又称为可变长子网掩码，当需要把大的网络划分为小的网络时，会用到 VLSM，以提高 IP 地址的利用率。

无类域间路由（Classless Inter-Domain Routing，CIDR）是一个在 Internet 上创建附加地址的方法，这些地址提供给服务提供商（ISP），再由 ISP 分配给客户。CIDR 将路由集中起来，使一个 IP 地址代表主要骨干提供商服务的几千个 IP 地址，从而减轻 Internet 路由器的负担。

IPv6 是“Internet Protocol Version 6”的缩写。IPv6 是互联网工程任务组（Internet Engineering Task Force，IETF）设计的用于替代现行版本 IP 协议（IPv4）的下一代 IP 协议。目前 IP 协议的版本号是 4（简称 IPv4），它的下一个版本就是 IPv6。

1. 三种通信模式

当前的网络中有三种通信模式：单播、广播和组播，其中的组播出现时间最晚，但同时具备单播和广播的优点，最具有发展前景。

(1) 单播

主机之间“一对一”的通信模式，网络中的交换机和路由器对数据只进行转发不进行复制。网络中的路由器和交换机根据其目标地址选择传输路径，将 IP 单播数据传送到其指定的目的地。

单播的优点主要有：

- ① 服务器及时响应客户机的请求。
- ② 服务器针对每个客户不同的请求发送不同的数据，容易实现个性化服务。

单播的缺点主要有：

- ① 服务器针对每个客户机发送数据流，服务器流量等于客户机数量×客户机流量；在客户数量大、每个客户机流量大的流媒体应用中服务器不堪重负。
- ② 现有的网络带宽是金字塔结构，城际、省际主干带宽仅仅相当于其所有用户带宽之和的 5%。如果全部使用单播协议，将造成网络主干不堪重负。

(2) 广播

主机之间“一对所有”的通信模式，网络对其中每一台主机发出的信号都进行无条件复制并转发，所有主机都可以接收到所有信息（不管你是否需要）。有线电视网就是典型的广播型网络，我们的电视机实际上是接收到所有频道的信号，但只将一个频道的信号还原成画面。在数据网络中也允许广播的存在，但其被限制在二层交换机的局域网范围内，禁止广播数据穿过路由器，防止广播数据影响大面积的主机。

广播的优点主要有：

- ① 网络设备简单，维护简单，布网成本低廉。
- ② 由于服务器不用向每个客户机单独发送数据，所以服务器流量负载极低。

广播的缺点主要有：

- ① 无法针对每个客户的要求和时间及时提供个性化服务。
- ② 网络允许服务器提供数据的带宽有限，客户端的最大带宽等于服务总带宽。
- ③ 广播禁止在 Internet 宽带网上传输。

(3) 组播

主机之间“一对一组”的通信模式，也就是加入了同一个组的主机可以接收到此组内的所有数据，网络中的交换机和路由器只向有需求者复制并转发其所需数据。主机可以向路由器请求加入或退出某个组，网络中的路由器和交换机有选择地复制并传输数据，即只将组内数据传输给那些加入组的主机。

组播的优点主要有：

- ① 需要相同数据流的客户端加入相同的组共享一条数据流，节省了服务器的负载。具备广播所具备的优点。
- ② 由于组播协议是根据接收者的需要对数据流进行复制转发，所以服务器端的服务总带宽不受客户接入端带宽的限制。

③ 此协议和单播协议一样允许在 Internet 宽带网上传输。

组播的缺点主要有：

① 与单播协议相比没有纠错机制，发生丢包错包后难以弥补，但可以通过一定的容错机制和 QoS 加以弥补。

② 现行网络虽然都支持组播的传输，但在客户认证、QoS 等方面还需要完善，这些缺点在理论上都有成熟的解决方案，只是需要逐步推广应用到现存网络当中。

2. IPv4 地址分类

IP 地址（IPv4）的长度为 32 位，分为网络号和主机号两部分。网络号标识一个网络，主机号用来标识网络中的一个主机。将 IP 地址分成了网络号和主机号两部分，就必须决定每部分包含多少位。网络号的位数直接决定了可以分配的网络数（计算方法： $2^{\text{网络号位数}}$ ）；主机号的位数则决定了网络中最大的主机数（计算方法： $2^{\text{主机号位数}}-2$ ）。将 IP 地址空间划分成不同的类别，每一类具有不同的网络号位数和主机号位数。正如图 9-1 所示，IP 地址的前 4 位用来决定地址所属的类别。

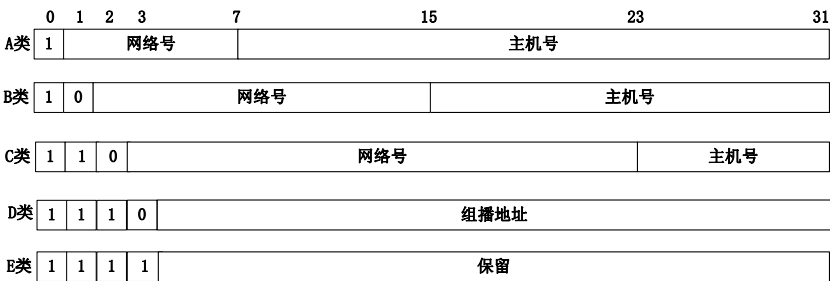


图 9-1 IP 地址分类示意图

① 网络地址：主机号全 0 表示网络地址（可做源、目标地址）。

② 子网广播地址：主机号全 1 表示广播地址（不能做源地址）。

③ 子网掩码：网络号部分全为 1，主机号部分全为 0；用于计算网络地址用（只需将 IP 地址和子网掩码做“与”操作，就可得到网络地址）。

④ 保留地址：为了满足内网的使用需求，保留了一部分不在公网使用的 IP 地址，如表 9-1 所示。

表 9-1 三类私有保留地址

类 别	IP 地址范围	网 络 号	网 络 数
A	10.0.0.0~10.255.255.255	10	1
B	172.16.0.0~172.31.255.255	172.16~172.31	16
C	192.168.0.0~192.168.255.255	192.168.0~192.168.255	255

⑤ 回送(Loopback)地址：为了方便测试，有一个表示本机的特殊保留地址，即 127.0.0.0。

3. IP 分配与子网划分

(1) 子网划分

在原先的 A、B、C 三类地址划分中，经常出现 B 类太大、C 类太小；或者是 B、C 类都太大的应用场景，因此就出现了“子网联网”和“可变成子网掩码（VLSM）”两种技术。

子网联网的主要思想就是将 IP 地址划分成三个部分：网络号、子网号和主机号。也就

是说，将原先的 IP 地址的主机号部分分成子网号和主机号两部分。说到底，也就是利用主机号部分继续划分子网。子网可以用“子网掩码”来识别。例如，我们可以将一个 C 类地址进行子网划分，如图 9-2 所示。

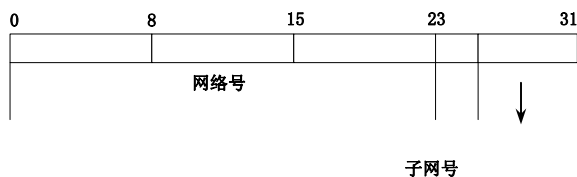


图 9-2 子网号示意图

将最后 8 位（原来的主机号），拿出两位用来表示子网，则可以产生“00”、“01”、“10”、“11”4 个子网。每个子网可包含 $2^6 - 2 = 62$ 个主机（6 代表剩余的主机位位数，有效变化值范围是 000001~111110，主机位不能全 0 也不能全 1，000000 代表网络，111111 代表广播被保留）。值得一提的是，这个时候，子网掩码就发生了变化，不再是 255.255.255.0（11111111 11111111 11111111 00000000），而是 255.255.255.192（11111111 11111111 11111111 11000000）。

在从 C 类地址中划分子网的时候，可以参照表 9-2 来进行。

表 9-2 子网划分

主机号中用于表示子网号的位数	子网划分后相对应的子网掩码	总共可用的子网地址数	每个子网可用的主机地址数
2 位	255.255.255.192	$2^2=4$	62
3 位	255.255.255.224	$2^3=8$	30
4 位	255.255.255.240	$2^4=16$	14
5 位	255.255.255.248	$2^5=32$	6
6 位	255.255.255.252	$2^6=64$	2

（2）VLSM

VLSM 是一种产生不同大小子网的网络分配机制。VLSM 用直观的方法在 IP 地址后面上加上“/网络及子网编码比特数”来表示。例如：192.168.123.0/26，就表示前 26 位表示网络号和子网号，即子网掩码为 26 位长，主机号 6 位长。利用 VLSM 技术，我们可以多次划分子网，即分完子网后，继续根据需要划分子网。

例如：某单位有 4 个部门，需建立 4 个子网，其中部门 1 有 50 台主机，部门 2 有 25 台主机，部门 3、4 则只有 10 台主机，有一内部 C 类地址：192.168.1.0。下面我们一起来看一下采用 VLSM 划分的过程。

首先，我们找到最大的网络：部门 1，需要 50 台主机。 $2^5 < 50 < 2^6$ ，因此至少需要 6 位主机号，剩下的 26 位则是网络号、子网号。而最后一个 8 位段还剩下 2 位，可以表示 00、01、10、11 这 4 个子网。因此得到：192.168.1.0/26、192.168.1.64/26、192.168.1.128/26、192.168.1.192/26 这 4 个子网。

假设我们将 192.168.1.64/26 分给部门 1，则现在就需要处理部门 2、3、4。这三个部门中部门 2 的网络最大，需要 25 台主机。 $2^4 < 25 < 2^5$ ，因此需要 5 位主机号，因此可以分成：192.168.1.128/27 和 192.168.1.160/27 两个子网。

然后，按这个思路划分下去，可以得到如表 9-3 所示的结果。

表 9-3 结果表

部 门	IP 地 址	网 络 范 围	主 机 数
部门 1	192.168.1.64/26	192.168.1.64~192.168.1.127	62
部门 2	192.168.1.128/27	192.168.1.128~192.168.1.159	30
部门 3	192.168.1.160/28	192.168.1.160~192.168.1.175	14
部门 4	192.168.1.176/28	192.168.1.176~192.168.1.191	14

注：网络范围中的前者是网络地址，后者是广播地址。

为了帮助大家参加考试时能够更快、更准确地计算出网络号/子网号、广播地址、可分配的网络/子网地址、有效子网号、主机数和子网数，下面对常见问题的解答技巧进行总结。

① 本子网划分，取网络号。A 类保留第一段 8 位组，后面全 0（如 IP 地址：10.1.0.0，网络号：10.0.0.0）；B 类保留前两段 8 位组，后面全 0（如 IP 地址：131.2.3.0，网络号：131.2.0.0）；C 类保留前三段 8 位组，后面全 0（如 IP 地址：192.168.1.5，网络号：192.168.1.0）。

② 复杂子网划分，取网络号。首先将掩码为 255 的部分对应照抄，然后对非 255 部分，将掩码和 IP 地址均转成二进制做与运算。例如：IP 地址为 192.168.1.100，子网掩码为 255.255.255.240，则前三个数都照抄，而最后一部分先转成二进制后再做与运算（0110 0100 AND 1111 0000 = 0110 0000，即 96），得到 192.168.1.96。

③ 给定 IP 地址和掩码，计算网络/子网广播地址。可根据规则：“网络/子网号是网络/子网中的最小数据字，广播地址是网络/子网中的最大数字值，网络中有效，可分配的地址则是介于网络/子网号和广播地址之间的 IP 地址”计算。

a. 基本子网划分，取广播地址。掩码为 255 的部分照抄，为 0 的部分改为 255。例如：IP 地址是 131.1.0.4，子网掩码为 255.255.0.0，则广播地址为 131.1.255.255。

b. 复杂子网划分，取广播地址。对于 255 部分照抄，0 部分转为 255，对于其他部分则先用 256 减去该值得到 x ，然后找到与 IP 地址中对应数最接近的 x 的倍数 y ，再将 $y-1$ 即可。例如：IP 地址是 131.4.101.129，子网掩码为 255.255.252.0，则首先将 255、255、_、0 的部分处理完，得到 131.4._.255，然后用 $256-252=4$ ，101 最接近的 4 的倍数是 104，因此得到广播地址为 131.4.103.255。

④ 根据复杂子网划分，获取有效子网数。例如：IP 地址是 140.140.0.0，子网掩码是 255.255.240.0，则先找到特别的掩码位 240，转换成二进制数 11110000，因此得知 IP 地址第三段 8 位组中主机位为有 4 位，用 2^4 为基数进行增长用以表示网络 ID：140.140.0.0，140.140.16.0，140.140.32.0，140.140.48.0，…，140.140.248.0。

（3）CIDR

CIDR（无类域间路由）是为了应对 VLSM 而产生的，它是一种路由技术，也就是说，如果你使用了 VLSM 技术进行子网划分，那么在互联时使用的路由器就必须能够支持 CIDR。因为如果区分各种类别的子网，那么就会使得路由表激增，而 CIDR 则采用了一种“最大匹配”的原则，可以有效地解决这个问题。

路由汇聚的含义是把一组路由汇聚为一个单个的路由广播。路由汇聚的最终结果和最明显的好处是缩小网络上的路由表的尺寸，这样将减少与每一个路由跳有关的延迟。由于减少了路由登录项数量，查询路由表的平均时间将加快。由于路由登录项广播的数量减少，路由协议的开销也将显著减少。随着整个网络（以及子网的数量）的扩大，路由汇聚将变得更加重要。

下面，我们通过一个例子来讲解路由汇聚算法的实现。

假设有 4 个路由：172.18.129.0/24、172.18.130.0/24、172.18.132.0/24 和 172.18.133.0/24，如果这 4 个路由进行路由汇聚，则能覆盖这 4 个路由的是：172.18.128.0/21。具体算法如下。

129 的二进制代码是 10000001，130 的二进制代码是 10000010，132 的二进制代码是 10000100，133 的二进制代码是 10000101。这 4 个数的前 5 位相同，都是 10000。所以加上前面的 172.18 这两部分相同的位数，网络号就是 $8+8+5=21$ （最大匹配原则）。而 10000000 的十进制数是 128。所以，路由汇聚的 IP 地址就是 172.18.128.0，最终答案就是 172.18.128.0/21。

(4) TCP/IP 端口

本知识点主要在于了解常用端口，熟知端口及其应用。

端口是传输层的内容，协议中低于 1024 的端口都有确切的定义，它们对应着 Internet 上常见的一些服务。这些常见的服务可以划分为使用 TCP 端口（面向连接）和使用 UDP 端口（无连接）两种。

类似于文件描述符，每个端口都拥有一个叫做端口号的整数描述符，用来区别不同的端口。由于 TCP/IP 传输层的 TCP 和 UDP 两个协议是两个完全独立的软件模块，因此，各自的端口号也相互独立。例如 TCP 有一个 255 号端口，UDP 也可以有一个 255 号端口，两者并不冲突。

按端口号进行划分，可分为 3 大类。

① 公认端口（Well Known Ports）：从 0 到 1023，它们紧密地绑定于一些服务。通常这些端口的通信明确表明了某种服务的协议。例如，80 端口实际上总是 HTTP 通信。

② 注册端口（Registered Ports）：从 1024 到 49151。它们松散地绑定于一些服务。也就是说，有许多服务绑定于这些端口，这些端口同样用于许多其他目的。例如，许多系统处理动态端口从 1024 左右开始。

③ 动态和/或私有端口（Dynamic and/or Private Ports）：从 49152 到 65535。理论上，不应为服务分配这些端口。实际上，机器通常从 1024 起分配动态端口。

常见的端口及其服务如表 9-4 所示。

表 9-4 常见的端口及其服务

端 口	服 务	端 口	服 务
20	文件传输协议（数据）	80	超文本传输协议（WWW）
21	文件传输协议（控制）	110	POP3 服务器（邮箱发送服务器）
23	Telnet 终端仿真协议	139	Win98 共享资源端口
25	SMTP 简单邮件发送协议	143	IMAP 电子邮件
42	WINS 主机名服务	161	SNMP – snmp
53	域名服务器（DNS）	162	SNMP-trap –snmp

4. IPv6 协议

本知识点在于掌握 IPv6 协议的主要特点，了解 IPv6 地址的格式，以及与 IPv4 地址的兼容性方案，了解 IPv6 相关的一些常识。

IPv6 在 IPv4 的基础上进行改进，它的一个重要的设计目标是与 IPv4 兼容。第一个 IPv6 标准被 IETF 接受并作为 RFC 发布不久，就产生了 6-bone 网络，在 IPv6 产品上实现广泛商业推广以前，用于测试或获取 IPv6 的经验。它也是中国第一个 IPv6 的商用网。

(1) 协议主要改进

IPv6 对 IPv4 的主要改进如下。

① 扩展地址。把原来 32 位地址扩展到 128 位，采用 16 进位表示，每 4 位构成一组，每组间用一个冒号隔开。为了更好地将 IPv4 过渡到 IPv6，IPv6 提供了两类嵌有 IPv4 地址的特殊地址如下。

0000:0000:0000:0000:0000:FFFF:xxxx:xxxx

0000:0000:0000:0000:0000:0000:xxxx:xxxx

其中 xxxx:xxxx 是原来的 IPv4 的 IP 地址。在 IPv6 中有两个特殊的地址：一个是全 0，表示未指定地址；另一个是 0:0:0:0:0:0:0:1，表示环回（Loopback）地址。

② 简化的包头。IPv6 的包头共有 8 个字段，总长为 40 字节；而 IPv4 的包头则包含至少 12 个字段，长度在没有选项时为 20 字节，有选项时达 60 字节。IPv6 采用固定格式的包头减少了需要检查和处理的字段的数量，提高选路效率。

③ 对扩展和选项支持的改进。IPv4 可以在 IP 的尾部加入选项，而 IPv6 则将选项加到单独的扩展头中。

④ 流标志。IPv4 对所有的包大致同等对待，这意味着每个包都是由中间路由器按照自己的方式来处理的，路由器并不跟踪任意两台主机间发送的包，因此不能“记住”如何对将来的包进行处理。而 IPv6 中引入了流概念，可以对流中的包进行高效处理。

⑤ 身份验证和保密。IPv6 使用了两种安全性扩展：IP 身份验证头、IP 封装安全性净荷。

(2) IPv6 报头结构说明

如图 9-3 所示，IPv6 协议对其报头定义了 8 个字段。

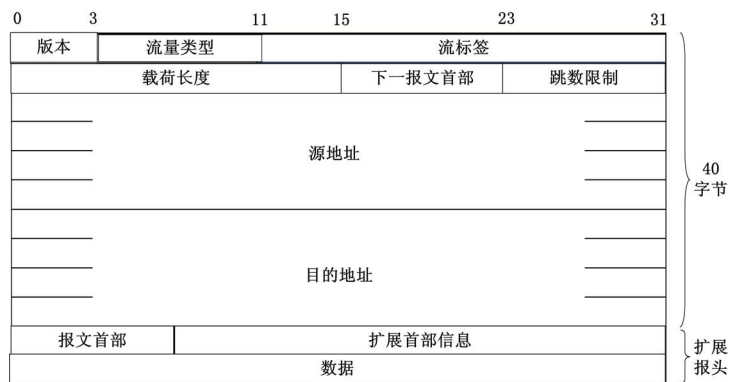


图 9-3 IPv6 报头格式示意图

① 版本：长度为 4 位，对于 IPv6，本字段的值必须为 6。

② 类别：长度为 8 位，指明为该包提供了某种“区分服务”。

③ 流标签：长度为 20 位，用于标识属于同一业务流的包（即特定源站到特定目的站），数据流的命名中包括流标签、源节点地址和目的节点地址。

④ 净荷长度：长度为 16 位，包括净荷的字节长度。

⑤ 下一个头：长度为 8 位，指出了 IPv6 头后所跟的头字段中的协议类型（指出高层是 TCP 还是 UDP）。

⑥ 跳极限：长度为 8 位，每转发一次该值减 1，到 0 则丢弃，用于高层设置其超时值。

⑦ 源地址：长度为 128 位，指出发送方的地址。

⑧ 目标地址：长度为 128 位，指出接收方的地址（可以是单播、组播或任意点播地址）。

(3) IPv6 地址表示

IPv6 地址为 128 位长，但通常写作 8 组每组 4 个十六进制数的形式。例如：2001:0db8:85a3:08d3:1319:8a2e:0370:7344 是一个合法的 IPv6 地址。

如果 4 个数字都是零，则可以被省略。例如：2001:0db8:85a3:0000:1319:8a2e:0370:7344 等价于 2001:0db8:85a3::1319:8a2e:0370:7344。

遵守这些规则，如果因为省略而出现了两个以上的冒号，则可以压缩为一个，但这种零压缩在地址中只能出现一次。因此以下地址：

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab

都是合法的地址，并且它们是等价的。同时前导的零可以省略，因此 2001:0DB8:02de::0e13 等价于 2001:DB8:2de::e13。

5. 互联网应用

本知识点在于从宏观概念上掌握 Internet 上的各种应用及 IIS 相关知识。

互联网上的应用层出不穷，本知识点主要是从宏观角度了解互联网上的一些典型应用，了解它们的主要特点。关于具体的知识与配置，会在后续章节中根据考试大纲的要求进行详细说明。

(1) DNS：域名服务，即实现 IP 地址与更易记的域名进行翻译转换的应用。

(2) E-mail：电子邮件，是现在数据量、使用量最大的一个互联网应用。常见的电子邮件协议有简单邮件传输协议（SMTP），用于邮件的发送与服务器间中继传输；邮局协议（POP），用于电子邮件的接收，现在常用的是第三版，简称 POP3；因特网消息访问协议（IMAP）也是一种用于接收信件的邮件协议。

(3) FTP：文件传输协议，是现在数据量最大的一个互联网应用。

(4) WWW：万维网，是现在互联网应用的核心应用。

(5) Gopher：互联网早期的一种全文检索服务，WWW 出现后它被取代。

(6) WebMail：是指利用浏览器通过 Web 方式来收发电子邮件的服务或技术。

(7) Usenet：新闻组是一个电子讨论组，可以在这里与遍及全球的用户共享信息以及对某些问题的看法。

(8) EZweb：是日本现有的 3 家手机上网服务之一，是目前世界上最广泛和成功的 WAP 服务。

(9) VOD：视频点播，通过视频压缩、流技术、组播协议实现。

(10) NetMeeting：网络会议，通过视频压缩、流技术、组播协议实现。

网站的建设是基于网站服务器的。在 UNIX 或 Linux 平台上，Apache 就是网站服务器。而对于 Windows NT/2000/2003 Server 来说，IIS 就是标准的网站服务器。IIS 是一种服务，

是 Windows 2000 Server 系列的一个组件。与其他 Windows 平台一样, Windows 2003 同样可以采用第三方软件或系统自带的 IIS 6.0 两种方式架设 Web 服务器。IIS 不同于一般的应用程序, 它就像驱动程序一样是操作系统的一部分, 具有在系统启动时被同时启动的服务功能。IIS 是允许在 Internet/Intranet 上发布信息的 Web 服务器, 通过 HTTP 传输信息, 还可配置 IIS 以提供 FTP 和其他服务, 如 NNTP 服务、SMTP 服务等。

IIS 在安全方面提供了几个新的特征: 摘要式身份验证、安全通信、服务器网关加密、安全向导、IP 地址及 Internet 域限制、Kerberos 6.0 身份验证协议兼容性、证书存储、Fortezza。

IIS 6.0 支持 WebDAV 和 ASP, 它有两个管理工具: 一个是用于 MMC 的 Internet Service Manager 外接程序, 另一个是基于 Web 浏览器管理的 Internet Service Manager。

9.2.2 一点一练

试题 1

IP 地址分为公网地址和私网地址, 以下地址中属于私网地址的是 (1)。

- (1) A. 10.216.33.124 B. 127.0.0.1 C. 172.34.21.15 D. 192.32.146.23

试题 2

如果子网 172.6.32.0/20 被划分为子网 172.6.32.0/26, 则下面的结论中正确的是 (2)。

- (2) A. 被划分为 62 个子网 B. 每个子网有 64 个主机地址
C. 被划分为 32 个子网 D. 每个子网有 62 个主机地址

试题 3

以下给出的地址中, 属于子网 172.112.15.19/28 的主机地址是 (3)。

- (3) A. 172.112.15.17 B. 172.112.15.14 C. 172.112.15.16 D. 172.112.15.31

试题 4

IPv6 地址分为 3 种类型, 它们是 (4)。

- (4) A. A 类地址、B 类地址、C 类地址 B. 单播地址、组播地址、任意播地址
C. 单播地址、组播地址、广播地址 D. 公共地址、站点地址、接口地址

试题 5

IPv6 地址 33AB:0000:0000:CD30:0000:0000:0000/60 可以表示成各种简写形式, 以下写法中, 正确的是 (5)。

- (5) A. A.33AB:0:0:CD30::/60 B. 33AB:0:0:CD3/60
C. 33AB::CD30/60 D. 33AB::CD3/60

试题 6

设有下面 4 条路由: 196.34.129.0/24、196.34.130.0/24、196.34.132.0/24 和 196.34.133.0/24, 如果进行路由汇聚, 能覆盖这 4 条路由的地址是 (6)。

- (6) A. 196.34.128.0/21 B. 196.34.128.0/22
C. 196.34.130.0/22 D. 196.34.132.0/23

试题 7

假设用户 Q1 有 2000 台主机, 则必须给他分配 (7) 个 C 类网络, 如果分配给用户 Q1 的超网号为 200.9.64.0, 则指定给 Q1 的地址掩码为 (8); 假设给另一用户 Q2 分配的 C 类网络号为 200.9.16.0~200.9.31.0, 如果路由器收到一个目标地址为 11001000 00001001 01000011 00100001 的数据报, 则该数据报应送给用户 (9)。

- (7) A. 4 B. 8 C. 10 D. 16

- (8) A. 255.255.255.0 B. 255.255.250.0 C. 255.255.248.0 D. 255.255.240.0
(9) A. Q1 B. Q2 C. Q1 或 Q2 D. 不可到达

试题 8

32 位的 IP 地址可以划分为网络号和主机号两部分。以下地址中, (10) 不能作为目标地址, (11) 不能作为源地址。

- (10) A. 0.0.0.0 B. 127.0.0.1
C. 10.0.0.1 D. 192.168.0.255/24
(11) A. 0.0.0.0 B. 127.0.0.1
C. 10.0.0.1 D. 192.168.0.255/24

试题 9

IPv6 的“链路本地地址”是将主机的 (12) 附加在地址前缀 1111111010 之后产生的。

- (9) A. IPv4 地址 B. MAC 地址 C. 主机名 D. 任意字符串

试题 10

ISP 分配给某公司的地址块为 199.34.76.64/28, 则该公司得到的地址数是 (13)。

- (10) A. 8 B. 16 C. 32 D. 64

9.2.3 解析与答案

试题 1 分析

公网地址由因特网信息中心 (Internet Network Information Center, Inter NIC) 负责。这些 IP 地址分配给注册并向 Inter NIC 提出申请的组织机构。通过它直接访问因特网。

私网地址属于非注册地址, 专门为组织机构内部使用。

它们之间最大区别是公网 IP 世界只有一个, 私有 IP 可以重复, 但是在一个局域网内不能重复。其中私网地址的范围为: 10.0.0.0~10.255.255.255; 172.16.0.0~172.31.255.255; 192.168.0.0~192.168.255.255。

试题 1 答案

- (1) A

试题 2 分析

子网 172.6.32.0/20 说明其子网的网络前缀为 20 位, 网络位为 12 位, 现在被划分为子网 172.6.32.0/26, 其网络前缀为 26 位, 主机位为 6 位, 就说明拿出了 6 位进行子网划分, 被划分为 2 的 6 次方个子网, 每个子网的主机地址为 2^6-2 , 为 62 个主机地址。

试题 2 答案

- (2) D

试题 3 分析

子网 172.112.15.19/28, 说明网络位为 28 位, 主机位为 4 位, 将其地址转换成二进制表示形式为: 172.112.15.00010011, 其网络地址为 172.112.15.00010000, 广播地址为 172.112.15.00011111, 所以其可用的主机范围为: 172.112.15.17~172.112.15.30。

试题 3 答案

- (3) A

试题 4 分析

IPv6 地址可分为以下三种。

单播地址：单播地址标示一个网络接口。协议会把送往地址的分组投送给其接口。单播地址包括可聚类的全球单播地址、链路本地地址等。

任播地址：也称泛播地址，任播地址用于指定给一群接口，通常这些接口属于不同的节点。若分组被送到一个任播地址时，则会被转送到成员中的其中之一。通常会根据路由协定，选择“最近”的成员。任播地址通常无法轻易分别，它们拥有和正常单播地址一样的结构，只是会在路由协定中将多个节点加入网络中。任播地址从单播地址中分配。

多播地址：也称组播地址。多播地址也被指定到一群不同的接口，送到多播地址的分组会被传送到所有的地址。

试题 4 答案

(4) B

试题 5 分析

IPv6 地址为 128 位长，但通常写作 8 组每组 4 个十六进制数的形式，例如，2001:0db8:85a3:08d3:1319:8a2e:0370:7344 是一个合法的 IPv6 地址。

如果 4 个数字都是零，可以被省略。例如：2001:0db8:85a3:0000:1319:8a2e:0370:7344 等价于 2001:0db8:85a3::1319:8a2e:0370:7344。

遵守这些规则，如果因为省略而出现了两个以上的冒号，则可以压缩为一个，但这零压缩在地址中只能出现一次。因此以下地址：

2001:0DB8:0000:0000:0000:0000:1428:57ab

2001:0DB8:0000:0000:0000::1428:57ab

2001:0DB8:0:0:0:0:1428:57ab

2001:0DB8:0::0:1428:57ab

2001:0DB8::1428:57ab

都是合法的地址，并且它们是等价的。同时前导的零可以省略，因此 2001:0DB8:02de::0e13 等价于 2001:DB8:2de::e13。

试题 5 答案

(5) A

试题 6 分析

路由汇聚的含义是把一组路由汇聚为一个单个的路由广播。路由汇聚的最终结果和最明显的好处是缩小网络上的路由表的尺寸，这样将减少与每一个路由跳有关的延迟。由于减少了路由登录项数量，查询路由表的平均时间将缩短。由于路由登录项广播的数量减少，路由协议的开销也将显著减少。随着整个网络（以及子网的数量）的扩大，路由汇聚将变得更加重要。

下面，我们通过一个例子来讲解路由汇聚算法的实现。

假设有 4 个路由：196.34.129.0/24、196.34.130.0/24、196.34.132.0/24 和 196.34.133.0/24，如果这 4 个路由进行路由汇聚，则能覆盖这 4 个路由的是：196.34.128.0/21。具体算法如下。

129 的二进制代码是 10000001，130 的二进制代码是 10000010，132 的二进制代码是 10001100，133 的二进制代码是 10001101。这 4 个数的前 5 位相同，都是 10000。所以加上前面的 196.34 这两部分相同的位数，网络号就是 $8+8+5=21$ （最大匹配原则）。而 10000000 的十进制数是 128。所以，路由汇聚的 IP 地址就是 196.34.128.0，最终答案就是 196.34.128.0/21。

试题 6 答案

(6) A

试题 7 分析

一个默认 C 类网络最多可以容纳 254 台主机，现在用户 Q1 有 2000 台主机，需要分配 $2000/254=8$ 个 C 类网络。如果分配给用户 Q1 的超网号为 200.9.64.0，子网掩码为 255.255.248.0，采用 CIDR 编址表示为 200.9.64.0/21，可以容纳 $2^{11}-2=2046$ 台主机。假设给另一用户 Q2 分配的 C 类网络号为 200.9.16.0~200.9.31.0，则用 CIDR 编址表示为：200.9.16.0/20，如果路由器收到一个目标地址为 11001000 00001001 01000011 00100001 的数据报，也就目的地址为 200.9.67.33，则该数据报应送给用户 Q1。

试题 7 答案

(7) B

(8) C

(9) A

试题 8 分析

32 位的 IP 地址可以划分为网络号和主机号两部分。各选项的地址中，0.0.0.0 不能作为目标地址，可以作为源地址使用，表示本网络上的本主机（详细参考 DHCP 过程）。网络号为 127 的非全 0 和全 1 的 IP 地址，用作本地软件回环测试之用（测试本机的 TCP/IP 软件是否安装正确），可以作为源地址和目的地址使用，主机号全为 1 的地址为广播地址，不能作为源地址使用，但可以作为目的地址使用。

试题 8 答案

(10) A

(11) D

试题 9 分析

IPv6 的“链路本地地址”是将主机的 MAC 附加在地址前缀 1111111010 之后产生的。

试题 9 答案

(12) B

试题 10 分析

ISP 分配给某公司的地址块为 199.34.76.64/28，说明其主机位为 4 位，则地址数为 $2^4=16$ 位。

试题 10 答案

(13) B

9.3 路由技术及路由协议

在路由技术及路由协议这个考点中，主要涉及静态路由、RIP 路由及配置、EIGRP 路由及配置和 OSPF 路由及配置这 4 方面的内容。

9.3.1 考点精讲

静态路由主要使用在小型的拓扑结构比较稳定的网络环境中。对于只有一个出口的企业环境通常都需要配置默认路由，默认路由还起到作为其他路由条目作备份的作用。但在大型网络中，通常都会使用动态路由，如 RIP、EIGRP、OSPF 等。

路由信息协议（RIP）是一种在网关与主机之间交换路由选择信息的标准。RIP 是一种内部网关协议。在国家性网络中，如当前的因特网，拥有很多用于整个网络的路由选择协议。

EIGRP 又称为增强型内部网关路由协议。它结合了链路状态和距离矢量型路由选择协议

的 Cisco 专用协议，采用弥散修正算法（DUAL）来实现快速收敛，可以不发送定期的路由更新信息以减少带宽的占用，支持 Appletalk、IP、Novell 和 NetWare 等多种网络层协议。

OSPF 又称为开放式最短路径优先路由协议。它是一个内部网关协议（Interior Gateway Protocol, IGP），用于在单一自治系统（Autonomous System, AS）内决策路由。与 RIP 相比，OSPF 是链路状态路由协议，而 RIP 是距离矢量路由协议。

1. 路由应用范围

根据路由选择协议的应用范围，可以将其分为内部网关协议、外部网关协议和核心网关协议三大类。其分类如图 9-4 所示。

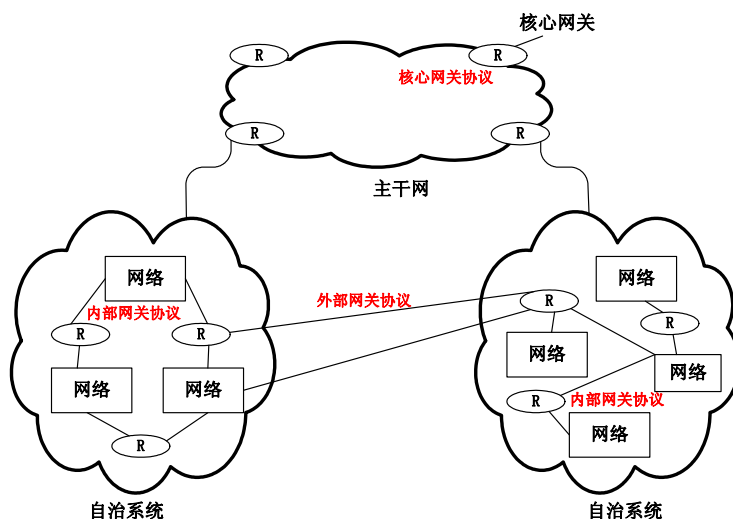


图 9-4 路由选择协议的应用范围

(1) 自治系统：是指同构型的网关连接的互联网络，通常是由一个网络管理中心控制的。

(2) 内部网关协议（IGP）：在一个自治系统内运行的路由选择协议，主要包括 RIP、OSPF、IGRP 和 EIGRP 等。

(3) 外部网关协议（EGP）：是指在两个自治系统之间使用的路由选择协议，最新的 EGP 协议是 BGP，其主要的功能是控制路由策略。

边界网关协议（BGP）是运行于 TCP 上的一种自治系统间路由协议。BGP 是唯一设计来处理因特网的大小的协议，也是唯一能够妥善处理非路由主机多路连接的协议。BGP 交互系统的主要功能是和其他的 BGP 系统交换网络可达信息。网络可达信息包括可达信息经过的自治系统（AS）清单上的信息。这些信息有效地构造了 AS 互联并由此清除了路由环路，同时在 AS 级别上实施了策略决策。

BGP 特点如下。

- ① 距离矢量协议。
- ② 传输协议：TCP，端口号为 17。
- ③ 支持 CIDR（无类别域间选路）。
- ④ 路由更新只发送增量路由。
- ⑤ 丰富的路由过滤和路由策略。

BGP-4 提供了一套新的机制支持无类域间路由。这些机制包括支持网络前缀的广播，取

消 BGP 网络中“类”的概念。BGP-4 也引入机制支持路由聚合，包括 AS 路径的聚合。这些改变为建议的超网方案提供了支持。

(4) 核心网关协议 (GGP)：Internet 中有个主干网，所有的自治系统都连接到主干网上，主干网中的网关称为核心网关，核心网关之间交换路由信息时使用的是核心网关协议。

我们常接触、使用得较多的路由选择协议是内部网关协议，根据算法的不同，主要包括 RIP、OSPF（开放最短路径优先）、IGRP（内部网关路由协议）、EIGRP（增强型内部网关路由协议）、IS-IS 5 种。路由选择协议将路由信息发送到其他节点所采用的基本算法是扩散法，为了避免信息重复发送，通常会对路由信息包进行编号，通常是每发送一个路由信息就递增编号（即加 1）。表 9-5 中总结了 5 种常见路由协议的知识点。

表 9-5 路由协议比较

协 议	类 别	主 要 特 点
RIP	距离向量协议	使用广泛，简单、可靠，支持 CIDR、VLSM 及连续子网，最大跳数是 15（隔一个路由器为一跳），每隔 30 秒广播一次路由信息。但其收敛慢，网络规模受限
IGRP	距离向量协议	使用组合用户配置尺度（包括延时、带宽、可靠性、负载），不支持 VLSM 和不连续子网，每 90 秒发送一次路由更新广播
OSPF	链路状态协议	通过路由器间通告网络接口状态（使用 LSA——链路状态通告）来建立链路状态数据库，生成最短路径树，每个路由器自己构造路由表。使用 Dijkstra 算法。主要优点是：迅速、无环路的收敛性、支持精确度量，但路由开销大
EIGRP	平衡混合（前两种）	使用一种散射更新算法，实现很高的路由性能。支持 VLSM、不连续子网，支持自动路由汇总功能，支持多种网络层协议
IS-IS	链路状态协议	能够应用于内部网关，也可用于外部网关

2. 路由协议分类

路由器可以使用两种基本方式进行路由选择：一是使用预先设置好的静态路由；二是使用一种动态路由选择协议来动态地计算路由。而动态路由选择协议根据实现机制的不同，又可以分为距离矢量路由选择、链路状态路由选择和混合路由选择三种类型。

(1) 静态路由

静态路由是预先设置的，将发现和传播路由的工作交给了互联网络管理者。

① 优点：有利于更安全的网络，能够更充分地利用资源，可以使用更小、更便宜的路由器。

② 缺点：当网络出现问题或其他原因引起拓扑变化时，需要管理员手工调整这些变化，在调整之前会因为无法识别失效的链路而造成路由失效。

③ 适用场合：非常小、到给定目标只有一条路径的网络；大型或复杂网络中的一个安全局部。

(2) 距离矢量路由

距离矢量路由定期给直接相邻的网络邻居传送它们路由选择表的副本，每个接收者将一个距离矢量（就是它自己的距离“值”）加到表中，并转发给它的邻居，以形成对网络“距离”的累积透视图。距离矢量路由主要包括 RIP、IGRP 两种。

① 优点：协议简单，易于配置、维护与使用。

② 缺点：当网络出现问题或其他原因引起拓扑变化时，路由器要花一定的时间来“汇聚”对新网络拓扑的认知，在这个过程中可能出现错误的问题。

③ 适用场合：适合于非常小的网络，这些网络没有或者有很少冗余路径，并且没有严格的网络性能要求。

（3）链路状态路由

链路状态路由支持关于网络拓扑结构的复杂数据库，通过与网络中其他路由器交换链路状态通知来实现。而且链路状态的交换是由网络中的一个事件触发的，而不是定期进行的，这样就可以加快汇聚的过程。链路状态路由主要包括 OSPF。

① 优点：具有良好的灵活性、扩展性。

② 缺点：在初始的发现过程中，有可能产生路由交换的泛滥，从而降低网络性能；并且对内存和处理器的要求高，使得路由器的费用提高。

③ 适用场合：适合任意大小的网络。

（4）混合路由

混合路由主要包括 EIGRP，综合了距离矢量路由和链路状态路由的优点。

3. 静态路由配置

所谓静态路由配置，也就是用户人为地指定对某一网络访问时所经过的路径。在图 9-5 中则列出了一个静态路由配置的例子。

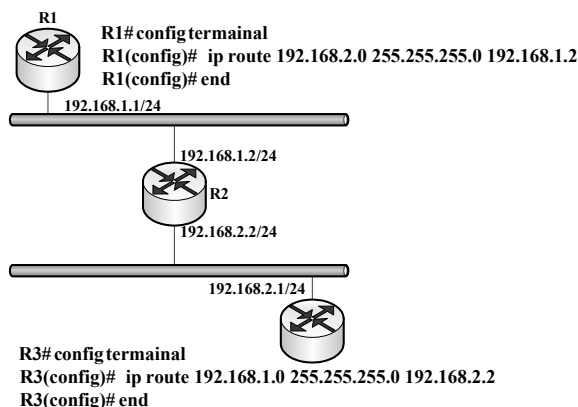


图 9-5 静态路由配置实例

其中最关键的配置语句是：Router(config)#ip route ip-addr subnet-mask gateway, ip-addr 为目的网络地址，subnet-mask 为目的网络地址子网掩码，gateway 为网关亦即到达目的网络的下一跳 IP 地址。

4. RIP 路由协议

RIP 采用距离矢量算法（常常归于 Bellman-Ford 或 Ford-Fulkerson 算法）计算路由，是最早的路由选择协议之一。RIPv2 还支持 CIDR（无类域间路由）和 VLSM（可变长子网掩码），它只适用于小型的同构网络，它是以跳数表示距离的（每经过一个路由器则跳数加 1），允许的最大跳数为 15，因此任何超过 15 个中间站点的目的地均被表示为不可达。RIP 是定期更新路由表的，它每隔 30 秒广播一次路由信息。

（1）RIP 路由配置常用命令

RIP 路由配置常用命令如表 9-6 所示。

表 9-6 RIP 路由配置常用命令

命 令	说 明
router rip	指定使用 RIP 协议
version {1 2}	指定 RIP 协议版本
no auto-summary	关闭自动汇总
network network-addr	指定与该路由器直接相连的网络
neighbor ip-addr	说明邻接路由器，以使它们能够自动更新路由
passive interface 接口	阻止在指定的接口发送路由更新信息
show ip route	查看路由表信息
show route rip	查看 RIP 协议路由信息

(2) RIP 配置实例

下面我们介绍一个网络的实例。

4 个位于不同地理位置的子网通过远程电缆连接在一起，现在要求使用 RIP 协议完成整个路由选择的配置，如图 9-6 所示。

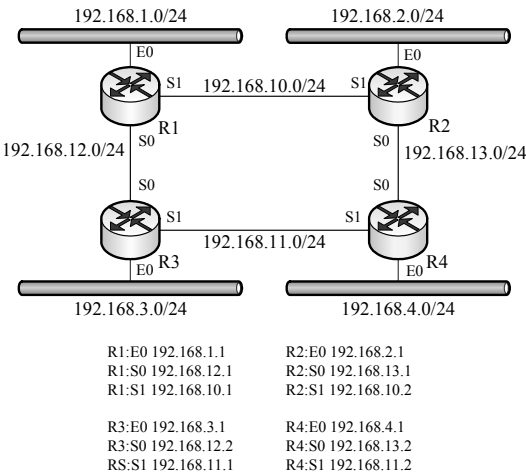


图 9-6 RIP 配置拓扑图

路由器 R1 的配置如下。

```
R1# config terminal                (进入全局配置模式)
R1(config)# router rip            (进入 RIP 协议配置子模式)
R1(config-router)# network 192.168.1.0 (说明路由器 R1 与 192.168.1.0 邻接)
R1(config-router)# network 192.168.10.0 (说明路由器 R1 与 192.168.10.0 邻接)
R1(config-router)# network 192.168.12.0 (说明路由器 R1 与 192.168.12.0 邻接)
R1(config-router)# version 2      (设置 RIP 的版本为 2)
R1(config-router)# no auto-summary (关闭接口自动汇总功能)
```

其他三个路由器的配置与此类似，只是根据其邻接网络的不同，修改相应的 network 子句即可。例如，路由器 R2 邻接的网络则是：192.168.2.0、192.168.10.0、192.168.13.0。

(3) RIP 协议路由信息

当完成了 RIP 路由选择协议的配置之后，我们可以使用 show ip route 命令来查看路由表

的信息。根据前面的配置，当我们查看 R1 的路由表时，将看到以下信息：

```
C 192.168.1.0 is directly connected,Ethernet0
C 192.168.12.0 is directly connected,Serial0
C 192.168.10.0 is directly connected,Serial1
R 192.168.2.0 [120/1] via 192.168.10.2,xx:xx:xx,Serial1
R 192.168.13.0 [120/1] via 192.168.10.2,xx:xx:xx,Serial1
R 192.168.3.0 [120/1] via 192.168.12.2,xx:xx:xx,Serial0
R 192.168.11.0 [120/1] via 192.168.12.2,xx:xx:xx,Serial0
R 192.168.4.0 [120/2] via 192.168.10.2,xx:xx:xx,Serial1
[120/2] via 192.168.12.2, xx:xx:xx, Serial0
```

第一部分，即最前面的 C 或 R 代表路由项的类别，C 是直连，R 代表是 RIP 协议生成的。

第二部分是目的网段。“[120/1]”表示 RIP 协议的管理距离为 120，1 则是路由的度量值，即跳数。我们可以看到路由器 R1 到 192.168.4.0 需要经过 R1→R2→R4 或 R1→R3→R4 两站，因此其度量值为 2，即两跳。

注：管理距离是用来表示路由协议的优先级的，RIP 的值为 120，OSPF 为 110、IGRP 为 100、EIGRP 为 90、静态设置为 1、直接连接为 0；因此我们可以看出在路由项中，EIGRP 是首选的，然后才是 IGRP、OSPF、RIP。

第三部分表示下一跳点的 IP 地址。

第四部分（xx:xx:xx）说明了路由产生的时间，以秒计算。

第五部分表示该条路由所使用的接口。

（4）RIP 路由更新的汇聚问题

RIP 的一大缺点就是当网络发生变化或出现故障而引起拓扑结构变化时，其汇聚完成是需要一定时间的。如图 9-7 所示的就是这样的一个例子。

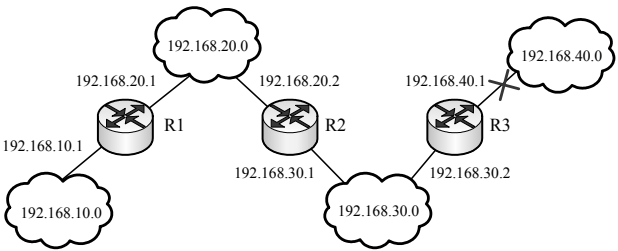


图 9-7 RIP 路由更新的汇聚问题

当一切正常时，各个路由器的路由表如表 9-7 所示。

表 9-7 各个路由器的路由表

目 的 网 络	R1		R2		R3	
	下一站地址	跳数	下一站地址	跳数	下一站地址	跳数
192.168.10.0	---（直连）	0	192.168.20.1	1	192.168.30.1	2
192.168.20.0	---（直连）	0	---（直连）	0	192.168.30.1	1
192.168.30.0	192.168.20.2	1	---（直连）	0	---（直连）	0
192.168.40.0	192.168.20.2	2	192.168.30.2	1	---（直连）	0

但如果这时路由器 R3 和网络 192.168.40.0 的连接发生了故障，就会路由更新，就会影响各个路由表，但由于 RIP 是定时更新（即每 30 秒更新一次），因此随着时间的不同，会有不同的结果。

表 9-8 中列出了在断开 30 秒及 500 秒后 R2 路由表的信息。

表 9-8 R2 路由表的信息

目的网络	R2（30 秒后）		R2（500 秒后）	
	下一站地址	跳数	下一站地址	跳数
192.168.10.0	192.168.20.1	1	192.168.20.1	1
192.168.20.0	---（直连）	0	---（直连）	0
192.168.30.0	---（直连）	0	---（直连）	0
192.168.40.0	192.168.20.1	3	---（不可达）	16

在 30 秒后，R2 收到了来自 R3 的路由更新信息——即 R3 已无法连接到 192.168.40.0 网段，但这时 R1 的路由表还没有更新，因此 R2 则认为其可以访问该网段，因此复制该路由表项，并将跳数加 1。随着不可达信息的蔓延，最终在 500 秒后，会使得跳数增长到 16，这时才真正完成了汇聚。

5. EIGRP 协议

EIGRP 是增强型的 IGRP 协议，是典型的平衡混合路由选择协议，融合了距离矢量和链路状态两种路由选择协议的优点，使用一种散射更新算法，实现了很高的路由性能。运行 EIGRP 的路由器之间形成邻居关系，并交换路由信息，通过 Hello 包维持邻居关系；它将存储所有与其相邻路由器的路由表信息，以快速适应路由变化。即在 EIGRP 路由器内包括：一个相邻路由器表、一个拓扑结构表和一个路由表。它支持 VLSM、自动路由汇总，支持多种网络层协议。

（1）EIGRP 路由配置常用命令

EIGRP 路由配置的常用命令如表 9-9 所示。

表 9-9 EIGRP 路由配置的常用命令

命令	说明
router eigrp autonomous-system	指定使用 EIGRP 协议，其中 autonomous-system 是自治系统号，EIGRP 协议只在相同自治系统号的路由器之间完成路由更新
network network-addr 掩码反码	指定与该路由器直接相连的网络。如果指定的网络是 A、B、C 类，则无须加入掩码反码；如果是子网，则需要加入掩码反码
no auto-summary	关闭自动汇总功能

（2）EIGRP 配置实例

EIGRP 配置拓扑图如图 9-8 所示。

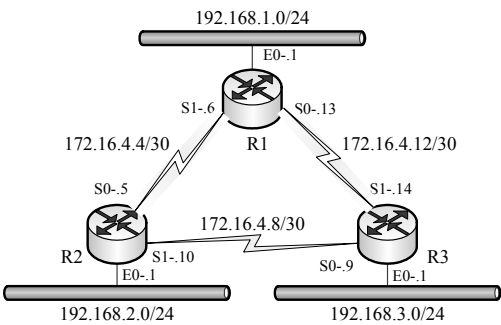


图 9-8 EIGRP 配置拓扑图

下面就以路由器 R1 为例，说明整个配置过程：

```
R1# config terminal                                (进入全局配置模式)
R1(config)# interface Ethernet0                    (进入以太网口 0 子配置模式)
R1(config)# ip address 192.168.1.1 255.255.255.0  (配置 IP 地址)
R1(config)# exit
R1(config)# interface Serial0                      (进入广域网口 0 子配置模式)
R1(config)# ip address 172.16.4.13 255.255.255.252 (配置 IP 地址)
R1(config)# bandwidth 1544                        (设置带宽)
R1(config)# exit
R1(config)# interface Serial1                      (进入广域网口 1 子配置模式)
R1(config)# ip address 172.16.4.6 255.255.255.252 (配置 IP 地址)
R1(config)# bandwidth 1544                        (设置带宽)
R1(config)# clockrate 130000                      (设置时钟频率)
R1(config)# exit
R1(config)# router eigrp 10                        (进入 EIGRP 协议配置子模式)
R1(config-router)# network 172.16.4.4 0.0.0.3
R1(config-router)# network 172.16.4.12 0.0.0.3
R1(config-router)# network 192.168.1.0
R1(config-router)# no auto-summary
```

注：在上面的配置中，network 172.16.4.4 和 172.16.4.12 是两个子网，因此需写出“掩码”的反码。也可以将其合并成为一句，即 network 172.16.0.0。

6. OSPF 路由协议

开放最短路径优先（OSPF）协议，和其他 SPF 一样，它采用的也是 Dijkstra 算法。OSPF 协议现在已成为最重要的路由选择协议之一，主要用于同一个自治系统。

OSPF 协议采用了“区域-area”的设计，提高了网络可扩展性，并且加快了网络汇聚时间。也就是将网络划分成许多较小的区域，每个区域定义一个独立的区域号并将此信息配置给网络中的每个路由器。从理论上说，通常不应该采用实际地域来划分区域，而是应该本着使不同区域间的通信量最小的原则进行合理分配。

（1）OSPF 路由配置常用命令

OSPF 路由配置的常用命令如表 9-10 所示。

表 9-10 OSPF 路由配置的常用命令

命 令	说 明
router ospf process-id	指定使用 OSPF 协议，其中 process-id 是其路由进程号，多个 OSPF 进程可以在同一个路由上配置，但通常不要这样做，该进程号只在路由器内部起作用，不同路由器可以不同
network 网码地址 掩码反码 area 区域号	指定与该路由器直接相连的网络。掩码反码可以用 255.255.255.255 减去掩码得到。区域号可以是数字，也可以是 IP 地址。ID 为 0 表示是主干域，不同网络区域的路由器通过主干域学习路由

续表

命 令	说 明
area 区域号 stub	将某区域转换成根区（不繁殖外部路由的区域）
show ip ospf neighbor	列出与本路由器是“邻居”关系（也就是进行路由信息交换的）的路由器
no ospf auto-cost-determination	OSPF 会自动根据每个接口的带宽，计算出其 cost（代价）： $\text{cost} = 10^8 / \text{带宽}$ （单位为 b/s）。
ip ospf cost	手动设置接口 cost

（2）OSPF 配置实例

下面我们以图 9-9 所示的一个网络为例说明 OSPF 路由选择协议的配置方法，该网络中有 0 和 1 两个区域，其中 R1 的 S1 端口、R2 的 S0 端口属于区域 0；而 R3、R1 的 S0 端口、R2 的 S1 端口则属于区域 1。

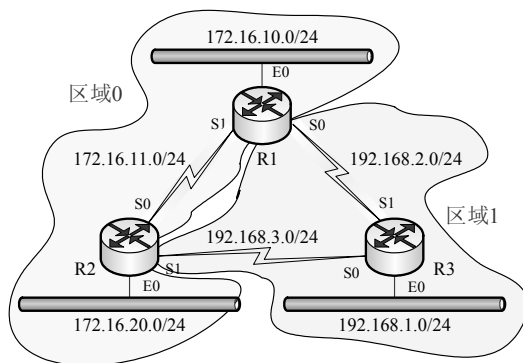


图 9-9 OSPF 配置拓扑图

下面列出 3 个路由器配置 OSPF 的指令。

```

R1# config terminal                                (进入全局配置模式)
R1(config)# router ospf 100                        (进入 OSPF 协议配置子模式)
R1(config-router)# network 172.16.10.1 0.0.0.0 area 0 (设置邻接网络)
R1(config-router)# network 172.16.11.1 0.0.0.0 area 0 (指定区域 0)
R1(config-router)# network 192.168.2.1 0.0.0.0 area 1
R2(config)# router ospf 200                        (进入 OSPF 协议配置子模式)
R2(config-router)# network 172.16.0.0 0.0.255.255 area 0 (设置邻接网络)
R2(config-router)# network 192.168.3.0 0.0.0.255 area 1
R3(config)# router ospf 300                        (进入 OSPF 协议配置子模式)
R3(config-router)# network 192.0.0.0 0.255.255.255 area 1 (设置邻接网络)

```

从上面的配置实例中我们可以知道，在配置 OSPF 时可以将子网进行合并，以减少条目，提高效率。例如 R3，其邻接子网是 192.168.1.0、192.168.2.0、192.168.3.0 三个，因此可以合并为 192.0.0.0/255.0.0.0；当然合并为 192.168.0.0/255.255.0.0 也是可行的。

7. 动态路由配置总结

虽然使用的路由选择协议不同，但是整个配置过程还是基本一致的，只是在具体的一些细节上有一些差别，只要掌握规律就不难记忆。表 9-11 给出了动态路由由协议配置的比较。

表 9-11 动态路由协议的配置比较

序 号	RIP	IGRP	OSPF	EIGRP
(1) 端口地址的基本设置	设置端口的网络地址	增加: clockrate bandwidth	与 RIP 相同	与 RIP 相同
(2) 开始设置路由	Ip routing	相同	相同	相同
(3) 指定路由选择协议	router rip	router igrp 100 (自治系统号)	router ospf 100 (OSPF 进程号)	router eigrp 200 (自治系统号)
(4) 说明邻接子网	network 子网号	network 子网号	network 子网号 子网掩码的反码 area 1	network 子网号 子网掩码的反码

注：子网掩码的反码的计算公式是“255.255.255.255-子网掩码”。

9.3.2 一点一练

试题 1

RIPv1 与 RIPv2 的区别是__(1)___。

- (1) A. RIPv1 是距离矢量路由协议，而 RIPv2 是链路状态路由协议
- B. RIPv1 不支持可变长子网掩码，而 RIPv2 支持可变长子网掩码
- C. RIPv1 每隔 30 秒广播一次路由信息，而 RIPv2 每隔 90 秒广播一次路由信息
- D. RIPv1 的最大跳数为 15，而 RIPv2 的最大跳数为 30

试题 2

OSPF 协议使用__(2)___报文来保持与其邻居的连接。下面关于 OSPF 拓扑数据库的描述中，正确的是__(3)___。

- (2) A. Hello B. Keepalive C. SPF D. LSU
- (3) A. 每一个路由器都包含了拓扑数据库的所有选项
- B. 在同一区域中的所有路由器包含同样的拓扑数据库
- C. 使用 Dijkstra 算法来生成拓扑数据库
- D. 使用 LSA 分组来更新和维护拓扑数据库

试题 3

RIP 是一种基于__(4)___算法的路由协议，一个通路上最大跳数是__(5)___，更新路由表的原则是到各个目标网络的__(6)___。

- (4) A. 链路状态 B. 距离矢量 C. 固定路由 D. 集中式路由
- (5) A. 7 B. 15 C. 31 D. 255
- (6) A. 距离最短 B. 时延最小 C. 流量最小 D. 路径最空闲

试题 4

为了限制路由信息传播的范围，OSPF 协议把网络划分成 4 种区域 (Area)，其中__(7)___的作用是连接各个区域的传输网络，__(8)___不接受本地自治系统之外的路由信息。

- (7) A. 不完全存根区域 B. 标准区域 C. 主干区域 D. 存根区域
- (8) A. 不完全存根区域 B. 标准区域 C. 主干区域 D. 存根区域

试题 5

以下关于边界网关协议 BGP4 的叙述中，不正确的是__(9)___。

- (9) A. BGP4 网关向对等实体 (Peer) 发布可以到达的 AS 列表
- B. BGP4 网关采用逐跳路由 (hop-by-hop) 模式发布路由信息
- C. BGP4 可以通过路由汇聚功能形成超级网络 (Supernet)

D. BGP4 报文直接封装在 IP 数据报中传送

试题 6

若路由器显示的路由信息如下，则最后一行路由信息是____(10)____得到的。

```
R3#show ip route
Gateway of last resort is not set
192.168.0.0/24 is subnetted, 6 subnets
C 192.168.1.0 is directly connected, Ethernet0
C 192.168.65.0 is directly connected, Serial0
C 192.168.67.0 is directly connected, Serial1
R 192.168.69.0 [120/1] via 192.168.67.2, 00:00:15, Serial1
[120/1] via 192.168.65.2, 00:00:24, Serial0
R 192.168.5.0 [120/1] via 192.168.07.2, 00:00:15, Serial1
R 192.168.3.0 [120/1] via 192.168.65.2, 00:00:24, Serial0
```

- (10) A. 串行口直接连接的 B. 由路由协议发现的
C. 操作员手工配置的 D. 以太网端口直连的

试题 7

某网络拓扑如图 9-10 所示，在主机 Host1 上设置默认路由的命令为____(11)____，在主机 Host1 上增加一条到服务器 Server1 主机路由的命令为____(12)____。

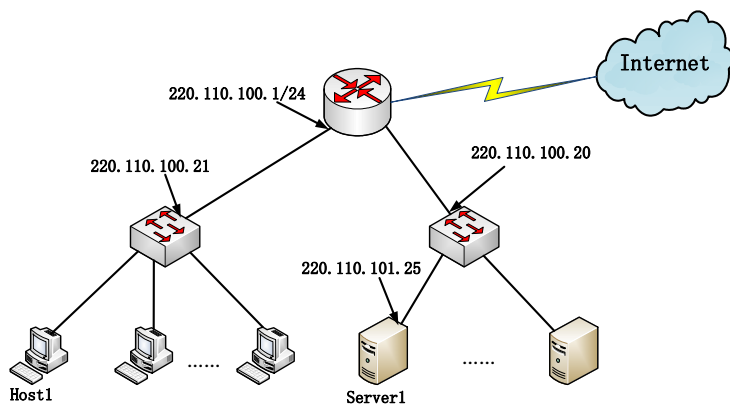


图 9-10 网络拓扑图

- (11) A. route add 0.0.0.0 mask 0.0.0.0 220.110.100.1
B. add 220.110.100.100.1 0.0.0.0 mask 0.0.0.0
C. add route 0.0.0.0 mask 0.0.0.0 220.110.100.1
D. add route 220.110.100.10.0:0.0 mask 0.0.0.0
- (12) A. add route 220.110.100.1 220.110.101.25 mask 255.255.255.0
B. route add 220.110.101.25 mask 255.255.255.0 220.110.100.1
C. route add 220.110.101.25 mask 255.255.255.255 220.110.100.1
D. add route 220.110.100.1 220.110.101.25 mask 255.255.255.255

试题 8

IGRP 协议的路由度量包括多种因素，但是在一般情况下可以简化为____(13)____。

- (13) A. 可靠性 B. 带宽 C. 跳步数 D. MTU

试题 9

OSPF 协议适用于 4 种网络。下面的选项中，属于广播多址网络的是____(14)____，属于非广播多址网络的是____(15)____。

- (14) A. Ethernet B. PPP C. Frame Relay D. RARP
(15) A. Ethernet B. PPP C. Frame Relay D. RARP

试题 10

RIP 协议默认的路由更新周期是____(16)____秒。

- (16) A. 30 B. 60 C. 90 D. 100

9.3.3 解析与答案

试题 1 分析

RIPv1 和 RIPv2 都采用距离矢量路由算法。RIPv1 利用 UDP 520 端口广播路由信息，路由信息中不包含子网掩码，所以不支持 CIDR。路由更新周期默认是 30 秒。如果在 180 秒内没有收到新的路由信息，就认为路由超时，再经过 120s 后该路由从表中删除。支持的最大跳数是 15，跳数 16 被认为是无穷大。RIPv2 在 RIPv1 的基础上增加了一些新特性如下：

- ① 报文认证功能。
- ② 支持可变长子网掩码 (VLSM) 和无类别域间路由 (CIDR)。
- ③ 采用组播地址 224.0.0.9 发送路由信息 (而不是广播)。

试题 1 答案

- (1) B

试题 2 分析

OSPF 共有以下 5 种分组类型。

类型 1：问候 Hello 分组，用来发现和维持邻站的可达性。

类型 2：数据库描述 DD 分组，向邻站给出自己的链路状态数据库中的所有链路状态项目的摘要信息。

类型 3：链路状态请求 LSR 分组，向对方请求发送某些链路状态项目的详细信息。

类型 4：链路状态更新 LSU 通告包，用洪泛法对全网更新链路状态。

类型 5：链路状态通告 LSA 分组，记录了链路状态变化信息的数据，封装在 LSU 中。

试题 2 答案

- (2) A (3) D

试题 3 分析

RIP 是一种基于距离矢量算法的路由协议，一个通路上最大跳数是 15，16 跳就认为不可达。更新路由表的原则是到各个目标网络的距离最短（跳数最少）。

试题 3 答案

- (4) B (5) B (6) A

试题 4 分析

OSPF 路由器使用其所在的不同区域进行身份标识，而 OSPF 区域类型通常有以下几种，这几种区域的主要区别在于它们和外部路由器间的关系。

① 标准区域：一个标准区域可以接收链路更新信息和路由总结。

② 主干区域（传递区域）：主干区域是连接各个区域的中心实体。主干区域始终是“区域 0”，所有其他的区域都要连接到这个区域上交换路由信息。主干区域拥有标准区域的所有性质。

③ 存根区域：存根区域是不接受自治系统以外的路由信息的区域。如果需要自治系统以外的路由，它使用默认路由 0.0.0.0。

④ 完全存根区域：它不接受外部自治系统的路由以及自治系统内其他区域的路由总结。需要发送到区域外的报文则使用默认路由 0.0.0.0。完全存根区域是 Cisco 自己定义的。

⑤ 不完全存根区域 (NSAA)：它类似于存根区域，但是允许接收以 LSA Type 7 发送的外部路由信息，并且要把 LSA Type 7 转换成 LSA Type 5。

区分不同 OSPF 区域类型的关键在于它们对外部路由的处理方式。外部路由由 ASBR 传入自治系统内，ASBR 可以通过 RIP 或者其他的路由协议学习到这些路由。

试题 4 答案

(7) C

(8) D

试题 5 分析

BGP 是一种路径矢量路由协议，用于传输自治系统间的路由信息，BGP 在启动的时候传播整张路由表，以后只传播网络变化的部分触发更新，它采用 TCP 连接传送信息，端口号为 179，在 Internet 上，BGP 需要通告的路由数目极大，由于 TCP 提供了可靠的传送机制，同时 TCP 使用滑动窗口机制，使得 BGP 可以不断地发送分组，而无须像 OSPF 或 EIGRP 那样停止发送并等待确认。

试题 5 答案

(9) D

试题 6 分析

第一部分，即最前面的 C 或 R 代表路由项的类别，C 是直连，R 代表是 RIP 协议生成的。第二部分是目的网段 192.168.3.0。“[120/1]”表示 RIP 协议的管理距离为 120，1 则是路由的度量值，即跳数。注：管理距离是用来表示路由协议的优先级的，RIP 的值为 120，OSPF 为 110、IGRP 为 100、EIGRP 为 90、静态设置为 1、直接连接为 0；因此我们可以看出在路由项中，EIGRP 是首选的，然后才是 IGRP、OSPF、RIP。第三部分 192.168.65.2 表示下一跳点的 IP 地址。第四部分 00:00:24 说明了路由产生的时间。第五部分 Serial0 表示该路由所使用的接口。

试题 6 答案

(10) B

试题 7 分析

route add 命令的主要作用是添加静态路由，通常的格式是：route add destination mask gateway interface，其中，destination 代表网段地址，mask 代表子网掩码，gateway 代表网关地址，例如在主机 Host1 上设置默认路由的命令，执行以下命令：route add 0.0.0.0 mask 0.0.0.0 220.110.100.1。在主机 Host1 上增加一条到服务器 Server1 的主机路由的命令为：route add 220.110.101:25 mask 255.255.255.255 220.110.100.1。

试题 7 答案

(11) A

(12) C

试题 8 分析

IGRP 度量标准的计算公式如下：

度量标准= $[K1 \times \text{带宽} + (K2 \times \text{带宽}) / (256 - \text{负载}) + K3 \times \text{延迟}] \times [K5 / (\text{可靠性} + K4)] \times 256$ ，默认的常数值为 $K1=K3=1$ ， $K2=K4=K5=0$ 。因此，IGRP 的度量标准计算简化为：度量标准= $(K1 \times \text{带宽} + K3 \times \text{延迟}) \times 256$ 。

试题 8 答案

(13) B

试题 9 分析

根据路由器所连接的物理网络不同, OSPF 将网络划分为 4 种类型: 广播多路访问型 (Broadcast MultiAccess)、非广播多路访问型 (None Broadcast MultiAccess, NBMA)、点到点型 (Point-To-Point)、点到多点型 (Point-To-MultiPoint)。广播多路访问型网络如 Ethernet、Token Ring、FDDI。NBMA 型网络如 Frame Relay、X.25、SMDS。Point-to-Point 型网络如 PPP、HDLC。

试题 9 答案

(14) A

(15) C

试题 10 分析

RIP 协议的路由更新原理是每隔一定时间 (默认为 30 秒) 发送一个路由更新消息, 以更新网络拓扑结构信息。当一台路由器收到一个 RIP 路由更新消息时, 这台路由器就会更新它自己的路由表, 以体现新的路由。

试题 10 答案

(16) A

9.4 NAT、ACL 及路由器常规配置

路由器 NAT、ACL 配置及常规配置这个考点中, 主要涉及路由器常规配置命令、NAT 工作原理和配置、ACL 工作原理和配置这三方面的内容。

9.4.1 考点精讲

路由器的常规配置包括模式切换、接口 IP 地址配置、使能口令配置等。

网络地址转换 (Network Address Translation, NAT) 属接入广域网 (WAN) 技术, 是一种将私有 (保留) 地址转化为合法 IP 地址的转换技术, 它被广泛应用于各种类型 Internet 接入方式和各种类型的网络中。原因很简单, NAT 不仅完美地解决了 IP 地址不足的问题, 而且还能够有效地避免来自网络外部的攻击, 隐藏并保护网络内部的计算机。

访问控制列表 (Access Control List, ACL) 是路由器和交换机接口的指令列表, 用来控制端口进出的数据报。ACL 适用于所有的被路由协议, 如 IP、IPX、AppleTalk 等。这张表中包含了匹配关系、条件和查询语句, 表只是一个框架结构, 其目的是为了对某种访问进行控制。

1. 路由器基本配置

路由器是一种典型的网络层设备, 在 OSI 参考模型中完成网络层中继或第三层中继的任务。路由器负责在两个局域网的网络层间传输数据分组, 并确定网络上数据传送的最佳路径 (选路协议、路由选择协议)。

(1) 访问路由器

访问路由器与访问交换机一样, 可以通过 Console (控制台) 端口连接终端或安装了终端仿真软件的 PC (第一次访问时必须采用), 或通过设备 AUX 端口连接 Modem, 或通过 Telnet, 或通过浏览器, 或通过网管软件这 5 种方式进行访问。

而使用 Console 端口连接的方式, 通常也是使用 “超级终端” 仿真软件, 并将端口的属性配置为: 端口速率——9600b/s, 数据位——8, 奇偶校验——无, 停止位——1, 流控——无。

（2）路由器的组成

与交换机一样，Cisco 路由器也有 4 种功能不同、材质不同的内存，用来存储引导软件的 ROM，用来保存 IOS 系统软件的 Flash，用来作为主存的 RAM，用来保存启动配置的 NVRAM。

在路由器中，也包括两份配置，一份是当前运行的（running-config），存储在 RAM 中的，表示为路由器当前生效的配置参数；另一份则是备份配置（start-config），存储在 NVRAM 中，每次启动时会自动装入。

（3）配置状态与转换命令

与交换机一样，Cisco 路由器也分为用户模式（登录时自动进入，只能够查看简单的信息）、特权模式（也称为 EXEC 模式，能够完成配置修改、重启等工作）、全局配置模式（对会影响 IOS 全局运作的配置项进行设置）和子配置模式（对具体的组件，如网络接口等进行配置）。4 种状态的转换命令如图 9-11 所示。

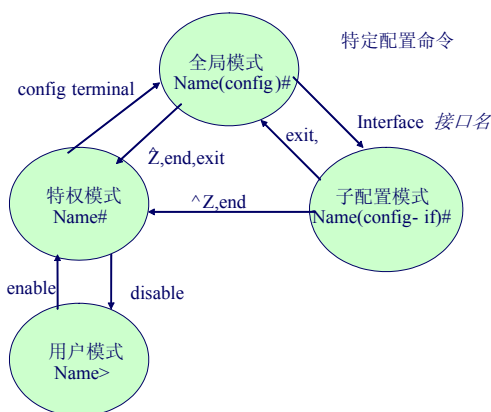


图 9-11 Cisco 路由器配置状态转换图

（4）路由器基本配置

① 配置 enable 口令和主机名

Router>	（用户模式提示符）
Router> enable	（进入特权模式）
Router #	（特权模式提示符）
Router # config terminal	（进入配置模式）
Router(config)#	（配置模式提示符）
Router(config)# enable password test	（设置 enable 口令为 test）
Router(config)# enable secret test2	（设置 enable 加密口令为 test2）
Router(config)# hostname R1	（设置主机名为 R1）
Router(config)# end	（退回特权模式）
R1#	

注：enable password 和 enable secret 只要配置一个就好，两者同时配置的情况下，后者生效。它们的区别在于，enable password 在配置项中是明文显示，而 enable secret 是密文显示。当用户敲入命令进入特权模式的时候，使用的密文特权口令方能进入特权模式。

② 接口基本配置

在 Cisco 路由器中通常是模块化的，每个模块都有一些相应的接口，例如以太网口、快速以太网口、串行口（Serial，即广域网口）等。而且与交换机不同，它们在默认情况下是关闭的，需要人为启动它。

```
Router> enable                                （进入特权模式）
Router # config terminal                      （进入配置模式）
Router(config)# interface fastethernet0/1    （进入接口 F0/1 子配置模式）
Router(config)# ip address 192.168.0.1 255.255.255.0
（设置该接口的 IP 地址，格式为：ip address ip-addr subnet-mask）
Router(config)# no shutdown                  （激活接口）
11:02:01:;%LINK-3-UPDOWN:Interface FastEthernet 0/1 changed state to up.
Router(config)# end                          （退回特权模式）
```

2. 网络地址转换

网络地址转换（NAT）的应用场景主要有两种：一是从安全角度考虑，不想让外部网络用户了解自己的网络结构和内部网络地址；二是从 IP 地址资源角度考虑，当内部网络人数太多时，可以通过 NAT 实现多台电脑共用一个合法 IP 访问 Internet。

NAT 设置可以分为静态地址转换、动态地址转换和复用动态地址转换 3 种。

（1）静态地址转换

静态地址转换将本地地址与合法地址进行一对一的转换，且需要指定和哪个合法地址进行转换。如果内部网络有 E-mail 服务器或 FTP 服务器等可以为外部用户提供的服务，这些服务器的 IP 地址必须采用静态地址转换，以便外部用户可以使用这些服务。整个配置过程包括 3 个步骤，如表 9-12 所示。

表 9-12 静态 NAT 配置

步 骤	功 能	命 令
1	在内部地址和合法地址之间建立静态转换（全局配置模式）	ip nat inside source static 内部地址合法地址
2	指定连接网络的内部端口	ip nat inside
3	指定连接外部网络的外部端口	ip nat outside

如图 9-12 所示的是一个静态 IP 地址转换的例子。

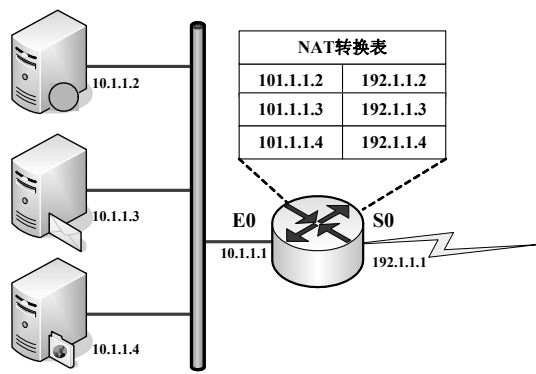


图 9-12 静态 IP 地址转换示例

```
ip nat inside source static 10.1.1.2 192.1.1.2
ip nat inside source static 10.1.1.3 192.1.1.3
ip nat inside source static 10.1.1.4 192.1.1.4
                                （手动设置静态的映射关系）
```

```
interface Ethernet0
ip address 10.1.1.1 255.255.255.0
ip nat inside                        （说明该端口是内网接口）
interface Serial0
ip address 192.1.1.1 255.255.255.0
ip nat outside                      （说明该端口是外网接口）
```

（2）动态地址转换

动态地址转换也是将本地地址与合法地址进行一对一的转换，但是动态地址转换是从合法地址池中动态地选择一个未使用的地址对本地地址进行转换。其配置包括 5 个步骤，如表 9-13 所示。

表 9-13 动态地址转换配置

步 骤	功 能	命 令
1	定义合法地址池（全局配置模式）	ip nat pool 地址池名称起始 IP 地址终止 IP 地址 子网掩码
2	定义一个标准的访问列表规则，指出允许哪些内部地址 可进行动态地址转换	access-list 标号 permit 源地址通配符 其中标号为 1~99 间的整数
3	将由访问列表指定内部地址与指定的合法地址池进行地 址转换	ip nat inside source list 访问列表标号 pool 地址 池名称
4	指定与内部网络相连的内部端口	ip nat inside
5	指定连接外部网络的外部端口	ip nat outside

对于如图 9-12 所示的例子，采用动态地址映射的配置如下所示。

```
ip nat pool PoolA 192.1.1.2 192.1.1.10 netmask 255.255.255.0
（设置合法地址池，名为 PoolA，地址范围是 192.1.1.2~192.1.1.10）
ip nat inside source list 1 pool PoolA
（对访问列表 1 中设置的本地地址，应用 PoolA 池进行动态地址转换）
interface Ethernet0
    ip address 10.1.1.1 255.255.255.0
    ip nat inside                        （说明该端口是内网接口）
interface Serial0
    ip address 192.1.1.1 255.255.255.0
    ip nat outside                      （说明该端口是外网接口）
access-list 1 permit 10.1.1.0 0.0.0.255 （10.1.1.0/24 的本地地址进行 NAT 转换）
```

（3）复用动态地址转换

复用动态地址转换首先是一种动态地址转换，但是它可以允许多个本地地址共用一个合法地址。对于只申请到少量 IP 地址，但却经常同时有多于合法地址个数的用户上外部网络的情况，这种转换极为有用。复用地址转换的配置如表 9-14 所示。

表 9-14 复用地址转换配置

步 骤	功 能	命 令
1	定义合法地址池（全局配置模式）	ip nat pool 地址池名称起始 IP 地址终止 IP 地址子网掩码
2	定义一个标准的访问列表规则，指出允许哪些内部地址可进行动态地址转换	access-list 标号 permit 源地址通配符 其中标号为 1~99 间的整数
3	在本地地址和合法 IP 地址间建立复用动态地址转换（与动态地址转换相比，就是加上 overload）	ip nat inside source list 访问列表标号 pool 地址池名称 overload
4	指定与内部网络相连的内部端口	ip nat inside
5	指定连接外部网络的外部端口	ip nat outside

假设在如图 9-12 所示的网络中，只有 2 个外部地址：192.1.1.1 和 192.1.1.2，显然不够用，因此就必须采用复用动态地址转换法。相比上一个而言，修改的只有其中的两句：

```
ip nat pool PoolA 192.1.1.1 192.1.1.2 netmask 255.255.255.0
```

（设置合法地址池，名为 PoolA，地址范围是 192.1.1.1~192.1.1.2）

```
ip nat inside source list 1 pool PoolA overload
```

（对访问列表 1 中设置的本地地址，应用 PoolA 池进行复用动态地址转换）

（4）IP 地址伪装

IP 地址伪装是另一种特殊的 NAT 应用，它是 M:1 的翻译，即用一个路由器的 IP 地址将子网中所有主机的 IP 地址都隐藏起来。如果子网中有多个主机要同时通信，那么还要对端口号进行翻译，所以也称为网络地址和端口翻译（NAPT）。该方法的特点是：

① 出去的数据报源地址被路由器的外部地址代替，而源端口号则被一个还未使用的伪装端口号代替。

② 进来的数据报的目标地址是路由器的 IP 地址，目标地址是其伪装端口号，由路由器进行翻译。

3. 访问控制列表（ACL）

访问控制列表用来限制使用者或设备，达到控制网络流量，解决拥塞，提高安全性等目的。在 IP 网络中，可以使用的访问列表有标准访问列表（值为 1~99）、扩展访问列表（标号为 100~199）两种。

（1）标准访问列表

功能说明：基于源 IP 地址来进行判定是否允许或拒绝数据报通过（或其他操作，例如在 NAT 中就是判断是否进行地址转换）。

命令格式：

```
access-list access-list-number {permit | deny}  
{source [source-wildcard] | any }
```

命令解释如下。

access-list：访问列表命令。

access-list-number: 访问列表号码, 值为 1~99。

permit: 允许。

deny: 拒绝。

source: 源 IP 地址。

source-wildcard: 源 IP 地址的通配符。

any: 任何地址, 代表 0.0.0.0 255.255.255.255。

通配符: **source-wildcard** 省略时, 则使用默认值 0.0.0.0。它的作用与子网掩码是不相同的, 当其取值为 1 时, 代表该位不必强制匹配; 当其取值为 0 时, 代表必须匹配。

因此, 如果 **source** 是 203.66.47.0, **source-wildcard** 是 0.0.0.255, 则说明只要前三组符合, 最后一组可以不符合, 即有一个 C 类的 IP 地址符合。

这个命令的实例如下:

access-list 1 permit host 202.1.2.3 (允许 IP 地址为 202.1.2.3 的数据报通过)

access-list 2 permit 202.1.2.0 0.0.0.255 (允许网络 202.1.2.0 的数据报通过)

access-list 3 deny host 202.1.2.3 (禁止 IP 地址为 202.1.2.3 的数据报通过)

access-list 5 deny 202. 1. 2.3

access-list 5 permit any

(标识为 5 的 ACL 有两条规则, 禁止 IP 地址为 202.1.2.3 的数据报通过, 但允许其他任何 IP 的数据报通过)

注: 制定好一个 ACL 的一条或多条访问规则后, 需要嵌套进设备的接口入或者出方向, ACL 方能真正意义生效。

其命令为: **(config-if)#ip access-group acl-num in|out**, ACL 应用到接口的入或出方向。

(2) 扩展访问列表

功能说明: 在标准访问列表的基础上增加更高层次的控制, 它能够基于目的地址、端口号码、对话层协议来控制数据报。

命令格式:

```
access-list access-list-number { permit | deny } {protocol \ protocol-keyword }  
{source [ source-wildcard ] | any } {destination destination-wildcard } | any }  
[ protocol-specific options] [ log ]
```

命令解释如下。

access-list-number: 访问列表号码, 值为 100~199。

protocol \ protocol-keyword: 可使用的协议, 包括 IP、ICMP、IGRP、EIGRP、OSPF 等。

destination destination-wild: 目的 IP 地址, 格式与源 IP 地址相同。

protocol-specific options: 协议指定的选项。

log: 记录有关数据报进入访问列表的信息。

这个命令的实例如下:

access-list 100 deny ip any 11.0.0.0 0.255.255.255

access-list 100 permit ip any any

(标识为 100 的扩展 ACL 禁止任何 IP 地址访问 11.0.0.0/8 网络的 IP 数据报, 允许其他的访问)

access-list 150 permit tcp any host 10.64.0.2 eq smtp

(允许以 SMTP 协议访问 10.64.0.2)

access-list 150 permit UDP any eq domain any (允许以任何 DNS 访问)

9.4.2 一点一练

试题 1

路由器命令 “Router(config)# access-list 1 deny 192.168.1.1” 的含义是____(1)____。

- (1) A. 不允许源地址为 192.168.1.1 的分组通过
- B. 允许源地址为 192.168.1.1 的分组通过
- C. 不允许目标地址为 192.168.1.1 的分组通过
- D. 允许目标地址为 192.168.1.1 的分组通过

试题 2

下面列出了路由器的各种命令状态, 可以配置路由器全局参数的是____(2)____。

- (2) A. router> B. router#
- C. router(config)# D. router(config-if)#

试题 3

路由器命令 Router>sh int 的作用是____(3)____。

- (3) A. 检查端口配置参数和统计数据 B. 进入特权模式
- C. 检查是否建立连接 D. 检查配置的协议

试题 4

配置路由器端口, 应该在____(4)____提示符下进行。

- (4) A. R1(config)# B. R1(config-in)# C. R1(config-intf)# D. R1(config-if)#

试题 5

以下 ACL 语句中, 含义为 “允许 172.168.0.0/24 网络所有 PC 访问 10.1.0.10 中的 FTP 服务” 的是____(5)____。

- (5) A. access-list 101 deny tcp 172.168.0.0 0.0.0.255 host 10.1.0.10 eq ftp
- B. access-list 101 permit tcp 172.168.0.0 0.0.0.255 host 10.1.0.10 eq ftp
- C. access-list 101 deny tcp host 10.1.0.10 172.168.0.0 0.0.0.255 eq ftp
- D. access-list 101 permit tcp host 10.1.0.10 172.168.0.0 0.0.0.255 eq ftp

试题 6

以下的访问控制列表中, ____ (6) ____ 禁止所有 Telnet 访问子网 11.11.1.0/24。

- (6) A. access-list 15 deny telnet any 11.11.1.0 0.0.0.255 eq 23
- B. access-list 115 deny udp any 11.11.1.0 eq telnet
- C. access-list 115 deny tcp any 11.11.1.0 0.0.0.255 eq 23
- D. access-list 15 deny udp any 11.11.1.0 255.255.255.0 eq 23

试题 7

关于路由器, 下列说法中正确的是____(7)____。

- (7) A. 路由器处理的信息量比交换机少, 因而转发速度比交换机快

router#config term	(进入配置模式命令)
router(config)#	(全局配置模式提示符)
router(config)#int f0/1	(进入接口配置模式)
route(config-if)#	(接口配置模式提示符)

试题 2 答案

(2) C

试题 3 分析

路由器命令 Router>sh int 的作用是检查端口配置参数和统计数据，全写为：Router>show interface。

试题 3 答案

(3) A

试题 4 分析

路由器的命令状态分为如下几种。

R1>：路由器处于用户命令状态，这时用户可以查看路由器的连接状态，访问其他网络和主机，但不能更改路由器配置的内容。

R1#：在“>”提示符下输入 enable，路由器进入特权命令状态，这时不但可以执行所有的用户命令，还可以看到和更改路由器的配置内容。

Router(config)#：在“#”提示符下输入 configure terminal，这时路由器处于全局配置状态，可以配置路由器的全局参数。

Router(config-if)#：端口配置状态。

Router(config-line)#：线路配置状态。

Router(config-router)#：路由协议配置状态。

在全局配置状态下，输入 interface type int/number subinterface，进入端口配置状态。输入 line type slo/ number，进入线路配置状态。输入 router protocol，进入路由协议配置状态。在路由器处于局部配置状态下，可以配置路由器的局部参数。

在开机后 60 秒内按 ctrl+break 键，路由器进入 RXBOOT 状态，这时路由器不能完成正常的功能，只能进行软件升级和手工引导。

试题 4 答案

(4) D

试题 5 分析

由于题目要求的是“允许”，因此命令中需要有 permit 关键词，而不能出现 deny 关键词。由于访问控制命令 access-list 的格式要求目标地址出现在源地址后面，这里选项 C、D 错在将源地址和目标地址写反，因此选择 B。

试题 5 答案

(5) B

试题 6 分析

访问控制列表分为标准访问控制列表，它只能对源地址做出判断，其表号标识范围是 1~99。另一种是扩展访问控制列表，可以对源地址、目的地址、源端口、目的端口和协议这 5 个要素作为判断依据，其表号标识范围是 100~199。根据题干要求禁止所有 Telnet 访问子网 11.11.1.0/24，只有扩展访问控制列表才能满足其要求。首先排除 A 和 D，A 和 D 的标号是 15，不满足扩展 ACL 的书写要求。Telnet 对应 TCP 协议的 23 号端口，所以只有 C 答案

是正确答案。

试题 6 答案

(6) C

试题 7 分析

路由器是一种网络层转发设备，它必须分拆数据帧，识别 IP 数据报中的目标地址字段，然后进行转发。多协议路由器通常能识别多种分组格式，所以用软件实现其转发功能，处理速度比交换机慢。路由器可以实现不同的服务质量，根据 IP 报头中 ToS 字段的编码选择不同可靠性、优先级、延迟或吞吐率的线路进行转发，所以不止是提供延迟最小的路由。不但能根据逻辑地址（即 IP 地址）进行转发，而且可以根据物理地址（通常是 MAC 地址）进行交换的设备叫三层交换机。

试题 7 答案

(7) C

试题 8 分析

在全局配置模式下用命令 `Router#setup` 进入设置对话状态（`setup mode`），利用设置对话状态可以避免手工输入命令的麻烦，但它不能完全代替手工配置，一些特殊的配置必须通过手工输入的方式完成。

在设置对话状态，路由器首先显示提示信息：

```
---System Configuration Dialog---  
At any point you may enter a question mark '?' for help.  
Use ctrl-c to abort configuration dialog at any prompt.  
Default settings are in square brackets '[]'.
```

然后，路由器就开始全局参数的配置：

```
Configuring global parameters
```

试题 8 答案

(8) D

试题 9 分析

题中的语句是一条标准 ACL 语句，表示允许源地址为 192.168.1.1 的分组通过，如果分组不匹配，则检查下一条语句。

试题 9 答案

(9) B

试题 10 分析

可以通过控制台端口来访问和配置路由器交换机。这也是最常用、最有效的配置方法。控制台端口（`Console`）是路由器的基本端口，连接控制台端口的线缆称为控制台电缆（`Console Cable`）。控制台电缆一端插入交换机的控制台端口，另一端插入 PC 的串行口，从而实现对交换机的访问和控制。并将端口的属性配置为：端口速率——9600b/s，数据位——8，奇偶校验——无，停止位——1，流控——无。

试题 10 答案

(10) C

9.5 网络系统建设

企业内部网络的建设已经成为提升企业核心竞争力的关键因素。企业网已经越来越多地

被人们提到,利用网络技术,现代企业可以在供应商、客户、合作伙伴、员工之间实现优化的信息沟通。这直接关系到企业能否获得关键的竞争优势。企业网络要求具有资源共享功能、通信服务功能、多媒体功能、远程 VPN 拨入访问功能。所以在进行企业网络的需求分析时,对企业的需求、应用范围、基于的技术等,要从企业应用角度来进行分析。

前期的网络规划对网络建设和使用至关重要。网络规划的任务就是为即将建立的网络系统提出一套完整的设想和方案,对建立一个什么形式、多大规模、具备哪些功能的网络系统做出全面科学的论证,并对建立网络系统所需的人力、财力和物力投入等做出一个总体的计划。

在网络系统建设这个考点中,主要涉及网络设计原则和网络设计步骤这两方面的内容。

9.5.1 考点精讲

在计算机网络设计和建设的工程实践中,科研人员总结了不少具体的设计经验和原则,对计算机网络可靠性的优化设计起到了较好的规范和指导作用,所以任何一个网络系统的建设都应该遵循相同的基本原则。

一个网络系统从构思开始,到最后被淘汰的过程被称为网络的生命周期,整个生命周期会有相应的建设步骤。一般来说,网络规模越大、投资越多,则其可能经历的循环周期也越多。

1. 网络设计原则

在网络设计方面,应着重考虑以下几个要素,它们也是网络设计和网络建设的基本原则。

(1) 采用先进、成熟的技术。在规划网络、选择网络技术和网络设备时,应重点考虑当今主流的网络技术和网络设备。只有这样,才能保证建成的网络有良好的性能,从而有效地保护建网投资,保证网络设备之间、网络设备和计算机之间的互联,以及网络的尽快使用、可靠运行。

(2) 遵循国际标准,坚持开放性原则。网络的建设应遵循国际标准,采用大多数厂家支持的标准协议及标准接口,从而为异种机、异种操作系统的互联提供极大的便利和可能。

(3) 网络的可管理性。对于具有良好的可管理性的网络,网管人员可借助先进的网管软件,方便地完成设备配置、状态监视、信息统计、流量分析、故障报警、诊断和排除等任务。

(4) 系统的安全性。一般的网络包括内部的业务网和外部网。对于内部用户,可分别授予不同的访问权限,同时对不同的部门(或工作组)进行不同的访问及连通设置。对于外部的互联网络,要考虑网络“黑客”和其他不法分子的破坏,防止网络病毒的传播。有些网络系统,如金融系统对安全性和保密性有着更加严格的要求。网络系统的安全性包括两个方面的内容,一方面是外部网络与本单位网络之间互联的安全性问题;另一方面是本单位网络系统管理的安全性问题。

(5) 灵活性和扩充性。网络的灵活性体现在连接方便,设置和管理简单、灵活,使用和维护方便等方面。网络的可扩充性表现在数量的增加、质量的提高和新功能的扩充等方面。网络的主干设备应采用功能强、扩充性好的设备,如模块化结构、软件可升级、信息传输速度快、吞吐量大。可灵活选择快速以太网、千兆以太网、FDDI、ATM 网络模块进行配置,关键元件应具有冗余备份的功能。

(6) 系统的稳定性和可靠性。选择网络产品和服务器时,最重要的一点应考虑它们的稳定性和可靠性,这也是我们强调选择技术先进、成熟的产品的重要原因之一。关键网络设备和重要服务器的选择应考虑是否具有好的电源备份系统、链路备份系统,是否具有中心处理模块的备份,系统是否具有快速、良好的自愈能力等。不应追求那些功能大而全但不可靠

或不稳定的产品，也不要选择那些不成熟和没有形成规范的产品。

(7) 经济性。网络的规划不但要保质保量按时完成，而且要减少失误、杜绝浪费。

(8) 实用性。网络设计一定要充分保护网络系统现有资源，同时要根据实际情况，采用新技术和新装备，还需要考虑组网过程要与平台建设及开发同步进行，建立一个实用的网络。力求使网络既满足目前需要，又能适应未来发展，同时达到较好的性价比。

2. 网络建设步骤

一个网络从立项、设计、采购、建设、调试到投入运行，是一项复杂的系统工程。如何减少失误、保护投资、提高效益，是工程建设过程中需要重点考虑的问题。网络的设计和施工必须有一整套完整的实施方法和步骤。良好的系统设计方法是保证系统成功的前提，一般要遵循如下步骤。

(1) 网络用户需求调查分析

网络需求分析的目的是充分了解组建网络应当达到的目标（包括近期目标和远期目标）。进行用户需求调研，需掌握以下几个方面的内容。

了解联网设备的地理分布，包括联网设备的数目、位置和间隔距离，用户群组织，以及特殊的需求和限制。

联网设备的软/硬件，包括设备类型、操作系统和应用软件等。

所需的网络服务，如电子邮件、WWW 服务、视频服务、数据库管理系统、办公自动化和 CMIS 系统集成等。

实时性要求、用户信息流量等。

本阶段的成果是提出网络用户需求分析报告。

(2) 系统可行性分析

系统可行性分析的目的是说明组建网络在技术、经济和社会条件等方面的可行性，以及评述为了合理地达到目标而可能选择的各种方案，并说明和论证最终选择的方案。本阶段的成果是提出可行性分析报告，供领导决策。

(3) 网络总体设计

网络总体设计就是根据网络规划中提出的各种技术规范 and 系统性能要求，以及网络需求分析的要求，制订出一个总体计划和方案。网络总体设计包括以下主要内容。

① 网络流量分析、估算和分配。

② 网络拓扑结构设计。

③ 网络功能结构设计。

本阶段的成果是确定一个具体的网络系统实施的总体方案，即网络的物理结构和逻辑关系结构。

(4) 网络详细设计

网络详细设计实质上就是分系统进行设计。一个网络由很多部分组成，我们把每个部分称为一个系统（或子系统），这样便于进行设计，能确保设计的精度。对于一个局域网而言，网络的详细设计包括以下内容。

① 网络主干设计。

② 子网设计。

③ 网络的传输介质和布线设计。

④ 网络安全和可靠性设计。

⑤ 网络接入互联网设计。

⑥ 网络管理设计，包括网络管理的范围、管理的层次、管理的要求，以及网络控制的能力。

⑦ 网络硬件和网络操作系统的选择。

(5) 设备配置、安装和调试

根据网络系统实施的方案，选择性价比高的设备，通过公开招标等方式和供应商签订供货合同，确定安装计划。

网络系统的安装和调试主要包括系统的结构化布线、系统安装、单机测试和互联调试等。在设备安装调试的同时开展用户培训工作。用户培训和系统维护是保证系统正常运行的重要因素，使用户尽可能地掌握系统的原理和使用技术，以及出现故障时的一般处理方法。

(6) 网络系统维护

网络组建完成后，还存在着大量的网络维护工作，包括对系统功能的扩充和完善，各种应用软件的安装、维护和升级等。另外，网络的日常管理也十分重要，如配置和变动管理、性能管理、日志管理和计费管理等。

9.5.2 一点一练

试题 1

网络系统设计过程中，逻辑网络设计阶段的任务是__ (1) __。

- (1) A. 依据逻辑网络设计的要求，确定设备的物理分布和运行环境
- B. 分析现有网络和新网络的资源分布，掌握网络的运行状态
- C. 根据需求规范和通信规范，实施资源分配和安全规划
- D. 理解网络应该具有的功能和性能，设计出符合用户需求的网络

试题 2

根据用户需求选择正确的网络技术是保证网络建立成功的关键，在选择网络技术时应考虑多种因素。下面各种考虑中，不正确的是__ (2) __。

- (2) A. 选择的网络技术必须保证足够的带宽，使得用户能快速地访问应用系统
- B. 选择网络技术时不仅要考虑当前的需求，而且要考虑未来的发展
- C. 越是大型网络工程，越是要选择具有前瞻性的新的网络技术
- D. 选择网络技术要考虑投入产出比，通过投入产出分析确定使用何种技术

试题 3

在网络设计阶段进行通信流量分析时可以采用简单的 80/20 规则，下面关于这种规则的说明中，正确的是__ (3) __。

- (3) A. 这种设计思路可以最大限度地满足用户的远程联网需求
- B. 这个规则可以随时控制网络的运行状态
- C. 这个规则适用于内部交流较多而外部访问较少的网络
- D. 这个规则适用的网络允许存在具有特殊应用的网段

试题 4

大型局域网络通常组织成分层结构（核心层、汇聚层和接入层），以下关于网络核心层的叙述中，正确的是__ (4) __。

- (4) A. 为了保障安全性, 应该对分组进行尽可能多的处理
- B. 将数据分组从一个区域高速地转发到另一个区域
- C. 由多台二、三层交换机组成
- D. 提供用户的访问控制

试题 5

网络设计过程包括逻辑网络设计和物理网络设计两个阶段, 各个阶段都要产生相应的文档, 以下选项中, (5) 属于逻辑网络设计文档, (6) 属于物理网络设计文档。

- | | |
|---------------------|----------------|
| (5) A. 网络 IP 地址分配方案 | B. 设备列表清单 |
| C. 集中访谈的信息资料 | D. 网络内部的通信流量分布 |
| (6) A. 网络 IP 地址分配方案 | B. 设备列表清单 |
| C. 集中访谈的信息资料 | D. 网络内部的通信流量分布 |

9.5.3 解析与答案

试题 1 分析

本题考查网络规划和设计的基础知识。网络逻辑设计阶段要根据网络用户的分类和分布, 选择特定的技术, 形成特定的网络结构。网络逻辑结构大致描述了设备的互联及分布情况, 但是并不涉及具体的物理位置和运行环境。逻辑设计过程主要由确定逻辑设计目标、网络服务评价、技术选项评价及进行技术决策 4 个步骤组成。

逻辑网络设计工作主要包括网络结构的设计、物理层技术选择、局域网技术选择与应用、广域网技术选择与应用、地址设计和命名模型、路由选择协议、网络管理和网络安全等内容。

试题 1 答案

(1) C

试题 2 分析

在网络设计方面, 应着重考虑以下几个要素, 它们也是网络设计和网络建设的基本原则。

① 采用先进、成熟的技术。在规划网络、选择网络技术和网络设备时, 应重点考虑当今主流的网络技术和网络设备。只有这样, 才能保证建成的网络有良好的性能, 从而有效地保护建网投资, 保证网络设备之间、网络设备和计算机之间的互联, 以及网络的尽快使用、可靠运行。

② 遵循国际标准, 坚持开放性原则。网络的建设应遵循国际标准, 采用大多数厂家支持的标准协议及标准接口, 从而为异种机、异种操作系统的互联提供极大的便利和可能。

③ 网络的可管理性。具有良好的可管理性的网络, 网管人员可借助先进的网管软件, 方便地完成设备配置、状态监视、信息统计、流量分析、故障报警、诊断和排除等任务。

④ 系统的安全性。一般的网络包括内部的业务网和外部网。对于内部用户, 可分别授予不同的访问权限, 同时对不同的部门(或工作组)进行不同的访问及连通设置。对于外部的互联网络, 要考虑网络“黑客”和其他不法分子的破坏, 防止网络病毒的传播。有些网络系统, 如金融系统对安全性和保密性有着更加严格的要求。网络系统的安全性包括两个方面的内容, 一方面是外部网络与本单位网络之间互联的安全性问题; 另一方面是本单位网络系统管理的安全性问题。

⑤ 灵活性和扩充性。网络的灵活性体现在连接方便, 设置和管理简单、灵活, 使用和维护方便等方面。网络的可扩充性表现在数量的增加、质量的提高和新功能的扩充等方面。网络的主干设备应采用功能强、扩充性好的设备, 如模块化结构、软件可升级、信息传输速度快、吞吐量大。可灵活选择快速以太网、千兆以太网、FDDI、ATM 网络模块进行配置, 关键元件应具有冗余备份的功能。

⑥ 系统的稳定性和可靠性。选择网络产品和服务器时，最重要的一点应考虑它们的稳定性和可靠性，这也是我们强调选择技术先进、成熟的产品的原因之一。关键网络设备和重要服务器的选择应考虑是否具有好的电源备份系统、链路备份系统，是否具有中心处理模块的备份，系统是否具有快速、良好的自愈能力等。不应追求那些功能大而全但不可靠或不稳定的产品，也不要选择那些不成熟和没有形成规范的产品。

⑦ 经济性。网络的规划不但要保质保量按时完成，而且要减少失误、杜绝浪费。

⑧ 实用性。网络设计一定要充分保护网络系统现有资源，同时要根据实际情况，采用新技术和新装备，还需要考虑组网过程要与平台建设及开发同步进行，建立一个实用的网络。力求使网络既满足目前需要，又能适应未来发展，同时达到较好的性价比。

试题 2 答案

(2) C

试题 3 分析

通信流量分布的简单规则 80/20 规则是指，对一个网段内部的通信流量，不进行严格的分布分析，仅仅是根据对用户和应用需求的统计，产生网段内的通信问题大小，总量的 80% 是在网段内部的流量，而 20% 是对网段外部的流量。80/20 规则适用于内部交流较多、外部访问相对较少、网络较为简单、不存在特殊应用的网络或网段。

试题 3 答案

(3) C

试题 4 分析

通常将网络中直接面向用户连接或访问网络的部分称为接入层，接入层目的是允许终端用户连接到网络，因此接入层交换机具有低成本和高端口密度特性；将位于接入层和核心层之间的部分称为分布层或汇聚层，汇聚层交换层是多台接入层交换机的汇聚点，它必须能够处理来自接入层设备的所有通信量，并提供到核心层的上行链路，因此汇聚层交换机与接入层交换机比较，需要更高的性能、更少的接口和更高的交换速率。而将网络主干部分称为核心层，核心层的主要目的在于通过高速转发通信，提供可靠的骨干传输结构，因此核心层交换机应拥有更高的可靠性、性能和吞吐量。

试题 4 答案

(4) B

试题 5 分析

这是一个考查网络设计过程的概念题，要求掌握每个过程所产生的文档的归类。其中逻辑网络设计包括以下几个：

- ① 网络总体设计，如分析目前的网络体系结构，网络逻辑结构等。
- ② 分层设计，如核心层、汇聚层、接入层的设计，以及连接到 Internet 的设计等。
- ③ IP 地址规划和设计。
- ④ 选路和路由。
- ⑤ 选择技术以及其他功能设计（聚合设计，冗余设计，安全设计）等。

而物理网络设计的主要是指结构化布线系统设计、网络机房系统设计和供电系统的设计等。

试题 5 答案

(5) A

(6) B

9.6 考前冲刺

试题 1

在以下网络应用中，要求带宽最高的应用是____(1)____。

- (1) A. 可视电话 B. 数字电视 C. 拨号上网 D. 收发邮件

试题 2

对路由选择协议的一个要求是必须能够快速路由收敛，所谓“路由收敛”是指____(2)____。

- (2) A. 路由器能把分组发送到预订的目标
B. 路由器处理分组的速度足够快
C. 网络设备的路由表与网络拓扑结构保持一致
D. 能把多个子网汇聚成一个超网

试题 3

以下的访问控制列表中，____(3)____禁止所有 Telnet 访问子网 10.10.1.0/24。

- (3) A. access-list 15 deny telnet any 10.10.1.0 0.0.0.255 eq 23
B. access-list 15 deny any 10.10.1.0 eq telnet
C. access-list 15 deny tcp any 10.10.1.0 0.0.0.255 eq 23
D. access-list 15 deny udp any 10.10.1.0 255.255.255.0 eq 23

试题 4

路由器的访问控制列表 (ACL) 的作用是____(4)____。

- (4) A. ACL 可以监控交换的字节数 B. ACL 提供路由过滤功能
C. ACL 可以检测网络病毒 D. ACL 可以提高网络的利用率

试题 5

一个局域网中某台主机的 IP 地址为 176.68.160.12，使用 22 位作为网络地址，那么该局域网的子网掩码为____(5)____。

- (5) A. 255.255.255.0 B. 255.255.248.0 C. 255.255.252.0 D. 255.255.0.0

试题 6

以下给出的地址中，属于子网 192.168.15.19/28 的主机地址是____(6)____。

- (6) A. 192.168.15.17 B. 192.168.15.14 C. 192.168.15.16 D. 192.168.15.31

试题 7

在一条点对点的链路上，为了减少地址的浪费，子网掩码应该指定为____(7)____。

- (7) A. 255.255.255.252 B. 255.255.255.248
C. 255.255.255.240 D. 255.255.255.196

试题 8

层次化网络设计方案中，____(8)____是核心层的主要任务。

- (8) A. 高速数据转发 B. 接入 Internet
C. 工作站接入网络 D. 实现网络的访问策略控制

试题 9

OSPF 协议使用____(9)____分组来保持与其邻居的连接。

- (9) A. Hello B. Keepalive
C. SPF (最短路径优先) D. LSU (链路状态更新)

试题 10

关于 OSPF 拓扑数据库, 下面选项中正确的是____(10)_____。

- (10) A. 每一个路由器都包含了拓扑数据库的所有选项
B. 在同一区域中的所有路由器包含同样的拓扑数据库
C. 使用 Dijkstra 算法来生成拓扑数据库
D. 使用 LSA 分组来更新和维护拓扑数据库

试题 11

以下协议中支持可变长子网掩码 (VLSM) 和路由汇总功能 (Route Summarization) 的是____(11)_____。

- (11) A. IGRP B. OSPF C. VTP D. RIPv1

试题 12

RIP 规定一条通路上最多可包含的路由器数量是____(12)_____。

- (12) A. 1 个 B. 16 个 C. 15 个 D. 无数个

试题 13

网络连接如图 9-13 所示, 要使计算机能访问到服务器, 在路由器 R1 中配置路由表的命令是____(13)_____。

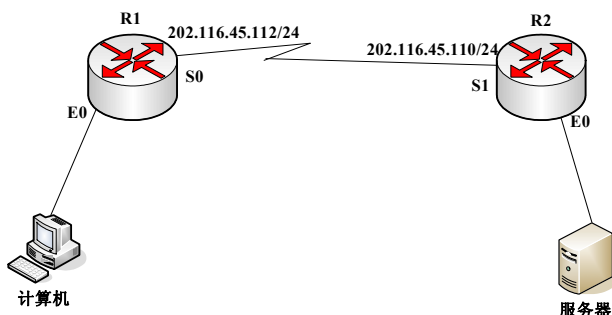


图 9-13 某网络拓扑图

- (13) A. R1(config)# ip host R2 202.116.45.110
B. R1(config)# ip network 202.16.7.0 255.255.255.0
C. R1(config)# ip host R2 202.116.45.0 255.255.255.0
D. R1(config)# ip route 201.16.7.0 255.255.255.0 202.116.45.110

试题 14

下列路由器协议中, ____ (14) ____ 用于 AS 之间的路由选择。

- (14) A. RIP B. OSPF C. IS-IS D. BGP

试题 15

按照网络分级设计模型, 通常把网络设计分为 3 层, 即核心层、汇聚层和接入层, 以下关于分级网络的描述中, 不正确的是____(15)_____。

- (15) A. 核心层承担访问控制列表检查功能
B. 汇聚层实现网络的访问策略控制
C. 工作组服务器放置在接入层
D. 在接入层可以使用集线器代替交换机

试题 16

把路由器配置脚本从 RAM 写入 NVRAM 的命令是____(16)_____。

- (16) A. save ram nvram B. save ram
C. copy running-config startup-config D. copy all

试题 17

如果要彻底退出路由器或者交换机的配置模式，输入的命令是____(17)_____。

- (17) A. exit B. no config-mode C. Ctrl+c D. Ctrl+z

试题 18

如果路由器配置了 BGP 协议，要把网络地址 133.1.2.0/24 发布给邻居，那么发布这个公告的命令是____(18)_____。

- (18) A. R1(config-route) #network 133.1.2.0
B. R1(config-route) #network 133.1.2.0 0.0.0.255
C. R1(config-route) #network-advertise 133.1.2.0
D. R1(config-route) #network 133.1.2.0 mask 255.255.255.0

试题 19

网络 122.21.136.0/24 和 122.21.143.0/24 经过路由汇聚，得到的网络地址是____(19)_____。

- (19) A. 122.21.136.0/22 B. 122.21.136.0/21
C. 122.21.143.0/22 D. 122.21.128.0/24

试题 20

设有下面 4 条路由：172.18.129.0/24、172.18.130.0/24、172.18.132.0/24 和 172.18.1330/24，如果进行路由汇聚，能覆盖这 4 条路由的地址是____(20)_____。

- (20) A. 172.18.128.0/21 B. 172.18.128.0/22
C. 172.18.130.0/22 D. 172.18.132.0/23

试题 21

属于网络 112.10.200.0/21 的地址是____(21)_____。

- (21) A. 112.10.198.0 B. 112.10.206.0 C. 112.10.217.0 D. 112.10.224.0

试题 22

在路由表中设置一条默认路由，目标地址应为____(22)_____。

- (22) A. 127.0.0.0 B. 127.0.0.1 C. 1.0.0.0 D. 0.0.0.0

试题 23

运行 OSPF 协议的路由器每 10 秒向它的各个接口发送 Hello 分组，接收到 Hello 分组的路由器就知道了邻居的存在。如果在____(23)_____秒内没有从特定的邻居接收到这种分组，路由器就认为那个邻居不存在了。

- (23) A. 30 B. 40 C. 50 D. 60

试题 24

关于外部网关协议 BGP，以下选项中，不正确的是____(24)_____。

- (24) A. BGP 是一种距离矢量路由协议 B. BGP 通过 UDP 发布路由信息
C. BGP 支持路由汇聚功能 D. BGP 能够检测路由循环

试题 25

在距离矢量路由协议中，可以使用多种方法防止路由循环，以下选项中，不属于这些方

法的是 (25)。

- (25) A. 垂直翻转 (flip vertical) B. 水平分裂 (split horizon)
C. 反向路由中毒 (posion reverse) D. 设置最大度量值 (metric infinity)

试题 26

设有下面 4 条路由：10.1.193.0/24、10.1.194.0/24、10.1.196.0/24 和 10.1.198.0/24，如果进行路由汇聚，覆盖这 4 条路由的地址是 (26)。

- (26) A. 10.1.192.0/21 B. 10.1.192.0/22 C. 10.1.200.0/22 D. 10.1.224.0/20

试题 27

通常路由器不进行转发的网络地址是 (27)。

- (27) A. 101.1.32.7 B. 192.178.32.2
C. 172.16.32.1 D. 172.35.32.244

试题 28

在网络 202.115.144.0/20 中可分配的主机地址数是 (28)。

- (28) A. 1022 B. 2046 C. 4094 D. 8192

试题 29

路由器 R1 的连接和地址分配如图 9-14 所示，如果在 R1 上安装 OSPF 协议，运行下列命令：router ospf 100，则配置 S0 和 E0 端口的命令是 (29)。

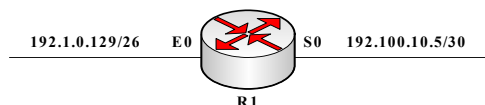


图 9-14 R1 互联拓扑

- (29) A. network 192.100.10.5 0.0.0.3 area 0
network 192.1.0.129 0.0.0.63 area 1
B. network 192.100.10.4 0.0.0.3 area 0
network 192.1.0.128 0.0.0.63 area 1
C. network 192.100.10.5 255.255.255.252 area 0
network 192.1.0.129 255.255.255.192 area 1
D. network 192.100.10.4 255.255.255.252 area 0
network 192.1.0.128 255.255.255.192 area 1

试题 30

某校园网的地址块是 138.138.192.0/20，该校园网被划分为 (30) 个 C 类子网，不属于该校园网的子网地址是 (31)。

- (30) A. 4 B. 8 C. 16 D. 32
(31) A. 138.138.203.0 B. 138.138.205.0 C. 138.138.207.0 D. 138.138.213.0

9.7 习题解析

试题 1 分析

本题考查网络应用占用带宽情况。

本题中，显然数字电视是要求带宽最高的，可视电话其次，可视电话采用 ISDN 业务实现，带宽也只需 128K，拨号上网仅仅 33.6Kb/s 的传输速率，而收发邮件对带宽基本没什么要求。考生在答题过程中最难区分的可能是数字电视与可视电话。

什么是数字电视, 数字电视的含义不仅是指我们一般人家中的电视接收机, 而是包含了从摄制、发送、传输到接收的全过程。摄像机摄制的节目经过电视台的后期制作后, 由电视台送出图像及声音信号, 经数字压缩和数字调制后, 形成数字电视信号, 经过空中无线方式或电缆有线方式传送, 由数字电视接收机接收后, 通过数字解调和数字视音频解码处理还原出原来的图像及伴音。因此, 数字电视就是在电视台播出节目和电视机接收节目全过程都采用数字技术进行处理的电视系统。

在传统的模拟电视中, 模拟全电视信号通过调制无线电射频载波上发送出去。广播信号可以是地面广播、有线电视网或卫星广播。数字电视则是将电视信号进行数字化采样, 其信号的数据率是很高, 演播室质量的数字化电视信号的数据率在 200Mb/s。要在原模拟电视频道宽带内传输如此高速率的数字信号是不可能的, 因此, 必须发展数据压缩技术。

实现数据压缩技术方法有两种: 一是信源编码过程中进行压缩, 利用人类听觉视觉效应去除信号中的多余成分, 在不影响收听收看效果的前提下尽量压缩数据率; 二是改进信道编码, 发展新的数字调制技术, 提高单位屏宽数据传送速率。在信源编码方面, IEEE 的 MPEG 专家组已发展制定了 ISO/IEC11172 (MPEG-1) 和 ISO/IEC13818 (MPEG-2) 两项国际标准。MPEG-1 的输入视频格式为 CIF352×288, 主要用于 CD-ROM、VCD 或 T1 (E1) 线路传输, 码率为固定的 1.5Mb/s; MPEG-2 供数字电视使用, 它支持标准分辨率的 16:9 宽屏及高清晰电视等多种格式, 其码率可变, 为 3~40Mb/s。

对于我国来说, 今后信源编/解码标准也会与美国、欧洲、日本一样采用 MPEG-2 标准。

试题 1 答案

(1) B

试题 2 分析

所谓“收敛”, 就是当路由环境发生变化后, 各路由器调整自己的路由表以适应网络拓扑结构的变化。“收敛”得越快, 路由器就越快适应网络拓扑结构的变化。

试题 2 答案

(2) C

试题 3 分析

访问控制列表 (ACL) 是应用在路由器接口的指令列表。随着网络应用及技术的日益发展, 在一些核心的路由交换机, 甚至边缘交换机上也应用了这一技术, 以期在网络的各个部分实现分布式的有效的控制。ACL 指令列表用来告诉路由器 (交换机) 哪些数据报可以接收、哪些需要拒绝。至于是接收还是被拒绝, 可以由类似源地址、目的地址、端口号等的特定条件来决定。而 TCP 支持 telnet 协议, 所以选 C。

试题 3 答案

(3) C

试题 4 分析

本题考查 ACL 的作用。

ACL 是对通过网络接口进入网络内部的数据报进行控制的机制, 分为标准 ACL 和扩展 ACL (Extended ACL) 两种。标准 ACL 只对数据报的资源地址进行检查, 扩展 ACL 对数据报中的资源地址、目的地址、协议以及端口号进行检查, 作为一种应用在路由器接口的指令列表, ACL 已经在一些核心路由交换机和边缘交换机上得到应用, 从原来的网络层技术扩展为端口限速、端口滤过、端口绑定等二层技术, 实现对网络的各层面的有效控制。

具体到安全领域来说, ACL 的作用主要体现在以下几个方面。

① 限制网络流量提高网络性能

通过设定端口上/下行流量的宽带，ACL 可以定制多种应用的宽带管理，避免因为宽带资源的浪费而影响网络的整体性能。如果能够根据宽带大小来制定收费标准，那么运营商就可以根据客户申请的宽带，通过启用 ACL 方式限定访问者的上/下行宽带，实现更好的管理，充分利用现有的网络资源，保证网络的使用性能。

② 有效的通信流量控制手段。

ACL 允许某一主机访问一个网络，阻止另一主机访问同样的网络，这种功能可以有效防止未经授权用户的非法介入。如果在边缘接入层启用二、三层网络访问的基本安全策略，ACL 能够将用户的 MAC、IP 地址、端口号与交换机的端口进行绑定，有效防止其他用户访问同样的网络。

B 答案比较勉强，因为 ACL 的主要功能在于控制访问，虽然通过 ACL 也可以做到路由过滤的功能。答案 A，ACL 不具备此功能，答案 C，ACL 可以防范某些病毒，但是不能检测。所以，本题选择答案 D。

试题 4 答案

(4) D

试题 5 分析

题中 22 位作为网络地址，子网掩码中 1 的个数就是 22，其掩码为：255.255.252.0 或/22。

试题 5 答案

(5) C

试题 6 分析

本题是一个子网划分的题目。

题干中 192.168.15.19/28 的子网掩码是 255.255.255.240。用 192.168.15.19 与 255.255.255.240 发生与运算得到 192.168.15.16/28 的网络 ID，在此网络 ID 下有效的主机 IP 地址是 192.168.15.17/28~192.168.15.30/28。显然 192.168.15.17 属于这个子网。只有 A 符合答案。B 不在其网络 ID 范围内，C 是网络地址，D 是该网络 ID 下的广播地址。

试题 6 答案

(6) A

试题 7 分析

子网掩码为 255.255.255.252 的地址访问总共只有 4 个地址，一个网络地址，一个广播地址，剩下两个地址分配给点对点的两个接口使用。B、C、D 选项浪费地址都过多。

试题 7 答案

(7) A

试题 8 分析

层次化网络设计在互联网组件的通信中引入了三个关键层的概念，这三个层次分别是核心层（Core Layer）、汇聚层（Distribution Layer）和接入层（Access Layer）。

① 核心层为网络提供了骨干组件或高速交换组件，在纯粹的分层设计中，核心层只完成数据交换的特殊任务。

② 汇聚层是核心层和终端用户接入层的分界面，汇聚层完成了网络访问策略控制、数据报处理，过滤，寻址，以及其他数据处理的任务。

③ 接入层向本地网段提供用户接入。

试题 8 答案

(8) A

试题 9 分析

OSPF 使用 hello 分组来发现相邻的路由器。当一个路由器启动时首先向邻接的路由器发送 hello 报文, 表明自己存在, 如有收到应答, 该路由器就知道了自己有哪些相邻的路由器。

试题 9 答案

(9) A

试题 10 分析

同一区域中的部分路由器有可能没有收到链路状态更新的数据报, 因此拓扑数据库就会不相同。

OSPF 使用溢流泛洪机制在一个新的路由区域中更新邻居 OSPF 路由器, 只有受影响的路由才能被更新; 发送的信息就是与本路由器相邻的所有路由器的链路状态; OSPF 不是传送整个路由表, 而是传送受影响的路由更新报文; OSPF 使用组播链路状态更新 (LSU) 报文实现路由更新, 并且只有当网络已经发生变化时才传送 LSU。

试题 10 答案

(10) D

试题 11 分析

本题考查提供 VLSM 和路由汇聚功能的协议的特性。

IGRP (Interior Gateway Routing Protocol) 是一种动态距离向量路由协议, 它由 Cisco 公司于 20 世纪 80 年代中期设计。使用组合用户配置尺度, 包括延迟、宽带、可靠性和负载。默认情况下, IGRP 每 90 秒发送一次路由更新广播, 如果在 3 个更新周期内 (即 270 秒), 没有从路由中的第一个路由接收到更新, 则宣布路由不可访问。在 7 个更新周期即 630 秒后, Cisco IOS 软件从路由表中清除路由, 与 RIPv1 一样都不支持 VLSM 和 CIDR。

VTP (VLAN Trunk Protocol), 即 VLAN 中继协议, 作用是交换机与交换机之间 VLAN 信息相互传递, 使用 VTP 协议可以在一个交换机中使用另一个交换机中 VLAN 配置信息, 从而避免了在不同交换机设置相同的 VLAN 所造成的重复劳动, 同时减少了 VLAN 配置错误的可能性。

4 个答案中, 只有 OSPF 支持 VLSM 和 CIDR。

试题 11 答案

(11) B

试题 12 分析

此题主要考查了 RIP 协议的特征。

RIP (路由选择信息协议) 是距离矢量路由协议的一种。所谓距离矢量是指路由器选择路由途径的评判标准: 在 RIP 选择路由的时候, 利用 D-V 算法来选择它所认为的最佳路径, 然后将其填入路由表, 在路由表中体现出来的就是跳数 (hop) 和下一跳的地址。

RIP 允许的最大站点数为 15, 任何超过 15 个站点的目的地址均被标为不可到达。所以 RIP 只适合于小型的网络。

试题 12 答案

(12) C

试题 13 分析

路由器配置路由信息的命令是 `ip route`。

通过配置静态路由，用户可以人为地指定对某一网络访问时所经过的路径，在网络结构比较简单，且一般到达某一网络所经过的路径唯一的情况下采用静态路由。

建立静态路由命令是：`ip route network mask address | interface [distance] [tag tag] [permanent]`。其中 Prefix 是指所要到达的目的网络；mask 是指子网掩码；address 是指下一个跳的 IP 地址，即相邻路由器的端口地址；interface 是指本地网络接口；distance 是指管理距离（可选）；tag tag 是指 tag 值（可选）；permanent 是指指定此路由即使该端口关掉也不被移掉。所以选 D。

试题 13 答案

(13) D

试题 14 分析

RIP、OSPF 和 IS-IS 都是内部网关协议，只有 BGP 用于 AS 之间的路由选择。

试题 14 答案

(14) D

试题 15 分析

网络分级设计把一个大的、复杂的网络分解为多个较小的、容易管理的网络。分级网络结构中的每一级解决一组不同的问题。在 3 层网络设计模型中，网络设备被划分为核心层、汇聚层和接入层。各层的功能如下。

核心层：尽快地转发分组，提供优化的、可靠的数据传输功能。

汇聚层：通过访问控制列表或其他过滤机制限制进入核心层的流量，定义了网络的边界和访问策略。

接入层：负责用户设备的接入，防止非法用户进入网络。

试题 15 答案

(15) A

试题 16 分析

把路由器配置脚本从 RAM 写入 NVRAM 的命令是：`copy running-config startup-config`。

试题 16 答案

(16) C

试题 17 分析

如果要彻底退出路由器或交换机的配置模式，输入的命令是 `Ctrl+z`。

试题 17 答案

(17) D

试题 18 分析

正确的命令应该是 `R1(config-route)#network 133.1.2.0 mask 255.255.255.0`。

试题 18 答案

(18) D

试题 19 分析

122.21.136.0/24 的二进制表示是 0111101000010101 10001000 00000000；

122.21.143.0/24 的二进制表示是 0111101000010101 10001111 00000000;
可以看出, 经过路由汇聚, 得到的网络地址是 122.21.136.0/21。

试题 19 答案

(19) B

试题 20 分析

172.18.129.0/24 的二进制表示是 10101100 00010010 10000001 00000000;
172.18.130.0/24 的二进制表示是 10101100 00010010 10000010 00000000;
172.18.132.0/24 的二进制表示是 10101100 00010010 10000100 00000000;
172.18.133.0/24 的二进制表示是 10101100 00010010 10000101 00000000;
这 4 条路由进行汇聚以后的 IP 地址为 172.18.128.0/21, 因此选 A。

试题 20 答案

(20) A

试题 21 分析

网络 112.10.200.0/21 的二进制表示是 01110000 00001010 11001000 00000000;
地址 112.10.198.0 的二进制表示是 01110000 00001010 11000110 00000000;
地址 112.10.206.0 的二进制表示是 01110000 00001010 11001110 00000000;
地址 112.10.217.0 的二进制表示是 01110000 00001010 11011001 00000000;
地址 112.10.224.0 的二进制表示是 01110000 00001010 11100000 00000000;
可以看出, 只有地址 112.10.206.0 与网络 112.10.200.0/21 满足最长匹配关系, 所以地址 112.10.206.0 属于 112.10.200.0/21 网络。

试题 21 答案

(21) B

试题 22 分析

在 RIP 协议中, 特殊地址 0.0.0.0 表示默认路径路由。当 RIP 更新报文中不便于罗列出所有的网络, 或者说当一个路由器要处理所有未明确列出的网络通信时, 可以使用默认路径路由。通常, 每个自治系统都有自己首选的默认路由, 0.0.0.0 项不会通过自治系统的边界。

试题 22 答案

(22) D

试题 23 分析

在 OSPF 路由器中, 默认的 Hello 报文时间间隔是 10 秒, 默认的无效时间间隔是 Hello 时间间隔的 4 倍。Hello 报文时间间隔可以通过命令 `ip ospf hello-interval` 更改, 无效时间间隔可以通过 `ip ospf dead-interval` 更改。

试题 23 答案

(23) B

试题 24 分析

BGP 协议是基于 TCP 协议之上的一种路由协议, 能够在各个自治系统之间传输路由信息。

试题 24 答案

(24) B

试题 25 分析

在 RIP 协议中,防止路由循环的第 1 种方法是假定 16 为路由度量的最大值。如果相互循环的过程使得路由度量达到 16,则路由器就认为链路或网络失效了,相应的路由表项作废。

防止路由循环的第 2 种方法是水平分裂法 (split horizon),也叫水平分割法。它是基于这样的规则:从某个接口学习到的路由条目不再从这个接口通告。

防止路由循环的第 3 种方法是反向路由中毒 (poison reverse),其规则为:如果路由器从一个接口学习到一条路由信息,那么应该向同一接口返回一条该路由不可达到的信息。

防止路由循环的第 4 种方法是触发更新 (triggered update)。正常情况下,路由更新消息每 30 秒发送一次。但是如果路由有改变,则立即发送更新信息。

试题 25 答案

(25) A

试题 26 分析

10.1.193.0/24 转化为二进制后的 IP 地址为: 00001010.00000001.11000001.00000000;

10.1.194.0/24 转化为二进制后的 IP 地址为: 00001010.00000001.11000010.00000000;

10.1.196.0/24 转化为二进制后的 IP 地址为: 00001010.00000001.11000100.00000000;

10.1.198.0/24 转化为二进制后的 IP 地址为: 00001010.00000001.11000110.00000000;

因此这 4 条路由进行路由汇聚后的 IP 地址为: 10.1.192.0/21, 备选答案中只有 10.1.192.0/21 包含此地址。

试题 26 答案

(26) A

试题 27 分析

通常路由器不进行转发的网络地址有: 10.x.x.x、172.16.x.x~172.31.x.x、192.168.x.x, 这些地址被大量用于企业内部网络中。一些宽带路由器,也往往使用 192.168.1.1 作为默认地址。私有网络由于不与外部互连,因而可能使用随意的 IP 地址。保留这样的地址供其使用是为了避免以后接入公网时引起地址混乱。使用私有地址的私有网络在接入 Internet 时,要使用地址翻译 (NAT) 将私有地址翻译成公用合法地址。在 Internet 上,这类地址是不能出现的。

试题 27 答案

(27) C

试题 28 分析

网络 202.115.144.0/20 的子网掩码中 1 的个数是 20,故可分配的主机地址数是: $2^{12}-2=4094$ 。

试题 28 答案

(28) C

试题 29 分析

配置动态 OSPF 路由器的命令如下:

```
Router> enable
Password:
Router# config terminal
Enter configuration commands one perline End with CNTL/Z
Routes config#routes ospf 1
```



```
Routes config-routes#network192.168.0.0 0.0.0.255 area 0.0.0.0
```

其中的 192.168.0.0 是子网的地址，也可以是路由器上的接口的 IP 地址或 OSPF 路由器所用接口的网络地址；而 0.0.0.255 掩码后面为 OSPF 所用的域。

试题 29 答案

(29) B

试题 30 分析

划分的 C 类子网为 $2^{24-20}=16$ 个。

分别将地址块 138.13 8.192.0/20 地址的第 3 个字节以及备选项 A、B、C、D 转化为二进制，即：

11000000, A: 11001011, B: 11001101, C: 11001111, D: 11010101。

第 3 个字节的前 4 位只有选项 A、B、C 和地址块一致，因此 D 不属于该校园网的子网地址。

试题 30 答案

(30) C

(31) D

网络管理技术是网络工程人员必备的职业技能。在工作中主要体现在网络管理体系的搭建,以及针对网管软件反馈的信息进行网络资源整合、网络性能分析、网络优化、网络故障排除等综合活动。

10.1 考点脉络

本章是网络工程师考试的一个必考点,根据考试大纲,要求考生掌握以下几个方面内容。

- (1) Windows 系统基本管理:主要考查文件系统、工作组和域管理模式。
- (2) Linux 系统基本管理:主要考查设备文件、用户权限、基本操作命令。
- (3) 网络参数配置:主要考查网络配置命令、常见网络配置文件及其解析。
- (4) 网络管理体系:主要考查网管体系、SNMP 协议。
- (5) 网络故障诊断:主要考查 Windows、Linux 系统下的诊断命令。
- (6) 网管工具和网络存储:主要考查 Sniffer 使用、数据备份与恢复、网络存储结构。

从历年的考试试题来看,本章的考点在综合知识考试中的平均分数为 5.2 分,约为总分的 6.9%。考试试题分数主要集中在网络操作系统基本管理、网络管理体系及网络故障诊断这 3 个知识点上。

10.2 网络操作系统基本配置

在网络操作系统基本配置这个考点中,主要涉及三个方面的知识,分别是 Windows 系统基本管理、Linux 系统基本管理和网络参数配置。

10.2.1 考点精讲

Windows 系统基本管理和 Linux 系统基本管理是分别基于 Windows 和 Linux 操作系统进行一系列诸如系统管理、磁盘管理、安全管理、网络参数配置管理、日志分析等活动,同时也是网络方向从业人员必备的一项基本技能。

通过前面的描述,网络参数配置管理也属于系统管理的一部分,但由于它又涉及网络互连和具体的参考命令(主要针对 Linux 系统),在这里单独作为一个知识点分析。

1. Windows 系统基本管理

下面主要介绍几种文件系统格式及其特性,API 调用,工作组、域与活动目录(AD)模型等相关知识点。

(1) 文件系统

本知识点在于让考生了解 Windows 常用的分区格式,分别是 FAT16、FAT32 和 NTFS

格式；Linux 操作系统的 4 种格式为 Ext2、Ext3、Linux Swap 和 VFAT，下面具体介绍。

① FAT16：文件分配表（File Allocation Table，FAT）的意义在于对硬盘分区的管理。以前用的 DOS、Windows 95 都使用 FAT16 文件系统，现在仍然在用的 Windows XP 系统支持 FAT16 文件系统。它最大可以管理 2GB 的分区，但每个分区最多只能有 65525 个簇。

② FAT32：随着大容量硬盘的出现，从 Windows 98 开始，FAT32 开始流行。它是 FAT16 的增强版本，可以支持大到 2TB（2048GB）的分区。FAT32 使用的簇比 FAT16 小，从而有效地节约了硬盘空间。

③ NTFS：新技术文件系统，是一种 Windows NT 内核的系列操作系统支持的、特别为网络和磁盘配额、文件加密等管理安全特性设计的磁盘格式。NTFS 也是以簇为单位来存储数据文件的，但 NTFS 中簇的大小并不依赖于磁盘或分区的大小。NTFS 可以支持更大的分区空间，速度更快，安全性更好（能够实现自动错误修复，可以实现文件级安全性），可以支持文件压缩功能。Windows 2000 之后的所有 Windows 系列操作系统都支持 NTFS 文件系统。

④ Ext2：可靠的 Linux 文件系统，但是没有元数据日志，这在启动系统时的 Ext2 文件系统的日常检查相当耗时。

⑤ Ext3：Ext2 文件系统的带日志版本，提供了元数据日志功能，目的是为了快速恢复数据，以及其他的增强日志模式，如全数据和有序数据日志。

⑥ Swap：Linux 中一种专门用于交换分区的 Swap 文件系统。Linux 是使用这一整个分区作为交换空间的。一般这个 Swap 格式的交换分区是主内存的两倍。在内存不够时，Linux 会将部分数据写到交换分区上。

⑦ VFAT：长文件名系统，这是一个与 Windows 系统兼容的 Linux 文件系统，支持长文件名，可以作为 Windows 与 Linux 交换文件的分区。

（2）API 调用

应用程序编程接口（Application Programming Interface，API）是一套用来控制 Windows 的各个部件（从桌面的外观到为一个新进程分配的内存）的外观和行为的一套预先定义的 Windows 函数。它是能用来操作组件、应用程序或者操作系统的一组函数、二次开发接口，开发人员可以根据 API 规定的软件接口，使用适当的语言和编程工具，利用软件产品和服务提供的数据和其他资源，遵循一定的规范，开发出新的软件产品和服务。

但是，没有合适的 Windows 编程平台，程序员想编写具有 Windows 风格的软件，必须借助 API，API 也因此被赋予至高无上的地位。然而随着软件技术的不断发展，在 Windows 平台上出现了很多优秀的可视化编程环境，程序员可以采用“所见即所得”的编程方式来开发具有精美用户界面和功能强大的应用程序。这些优秀的可视化编程环境操作简单、界面友好（诸如 VB、VC++、Delphi 等），在这些工具中提供了大量的类库和各种控件，它们替代了 API 的神秘功能，事实上这些类库和控件都是构架在 Win32 API 函数基础之上的，是封装了的 API 函数的集合。它们把常用的 API 函数组合在一起成为一个控件或类库，并赋予其方便的使用方法，所以极大地加快了 Windows 应用程序开发的过程。有了这些控件和类库，程序员便可以把主要精力放在程序整体功能的设计上，而不必过于关注技术细节。

实际上，如果要开发出更灵活、更实用、更具效率的应用程序，必然要直接使用 API 函数，虽然类库和控件使应用程序的开发变得简单很多，但它们只提供 Windows 的一般功能，对于比较复杂和特殊的功能来说，使用类库和控件是非常难以实现的，这时就需要采用 API 函数来实现。

（3）工作组、域与活动目录

本知识点主要需要考生了解工作组、域与活动目录的相关概念及特性。

① 工作组

Windows 工作组是一组由网络通信设备和介质互连在一起的计算机，它们分散在网络上，每一台计算机既可以是工作站，也可以是服务器；可以有自己的用户账号，也可以访问授权的计算机资源或将自己的资源共享给其他计算机。工作组式的网络结构是分布式的管理模式，工作组中的任何一台计算机只负责管理本地的资源，主机可以任意地加入或退出某一工作组（workgroup 为默认组）。

② 域与活动目录

域模式的网络结构是集中式的管理模式，网络中的任何一台计算机都可以加入一个域中，但必须经过域管理员的批准，属于网络的资源统一由域控制器来负责管理。工作组模式适合小型、分散型的网络；域模式适合较大型的、集中的网络。与工作组的“松散会员制”有所不同，“域”是一个相对严格的组织。“域”指的是由服务器控制网络上的计算机能否加入的计算机组合。

域模型是 **Windows** 系统中将网络管理和安全性策略集中的方案。每个域都有一台主域控制器（PDC，负责保存域中所有用户账号、组以及安全设置等数据）和归属的工作站，当域的规模较大时，可以安装备份域控制器来缓解。

对于较小规模的网络，只需要设置一个域即可，其称为单域模型；而如果网络规模较大，则可以分成多个域，而根据域的管理可以分为 3 种，如表 10-1 所示。

表 10-1 域的管理模型

域 模 型	主 域 个 数	账 户 管 理	信 任 关 系
主域模型	1 个	主域是账户域	其他域均信任该域
多主域模型	少量	所有网络账户均建立在其中一个主域上	主域间相互信任
完全信任模型	多个	分离	域间完全信任

而在 **Windows 2000** 操作系统中放弃了 NT 中的域管理方式，采用目录管理技术，即活动目录——AD 服务（**Windows 2000** 之后的 WIN 2003、WIN2008、WIN2012 都很好地支持 AD 服务）。AD 是基于 LDAP 格式的系统而设计的，它以对象的形式存储关于网络元素的信息，提供完全树状层次视图。AD 中对象模型称为架构，用来定义对象的类别与属性的描述。AD 的逻辑单元包括域（核心单元，是容器对象，可以包括计算机、用户等这些基本对象）、组织单元（用于将域内的对象组织成逻辑组）、域树（域的集合）、域林（域树的集合，用信任关系相关联）。域林包括域树，域树由域组成，域由各个基本对象组成，而且可以分成不同的组织单元。

2. Linux 系统基本管理

本知识点重点在于让考生了解 UNIX 与 Linux 的特点，熟悉常用的命令，掌握网络配置命令与常用配置文件等。

（1）设备文件

Linux 文件系统包括：文本文件、二进制文件、目录文件、连接文件、设备文件和管道文件（用于进程间通信）。网络工程师考试主要考查设备文件相关知识。**Linux** 将外设看做一个文件来管理，用户使用外设就像使用普通文件一样。设备文件存放在/dev 目录下，它使用设备的主设备号和次设备号来区分指定的外设。主设备号说明设备类型，次设备号说明具体

指哪一个设备。Linux 下的/dev 目录中有大量的设备文件，主要是块设备文件和字符设备文件，如表 10-2 所示。

表 10-2 设备文件标识

设备标识分解	表示内容	举例说明
前两个字母	分区所在设备类型	Hd: IDE 硬盘; Sd: SCSI 硬盘; Fd: 软盘
第三个字母	分区在哪个设备上	Hda: 第一块 IDE 硬盘; Hdb: 第二块 IDE 硬盘; Hdc: 第三块 IDE 硬盘
数字	分区序号	数字 1~4 表示主分区或扩展分区，逻辑分区从 5 开始
例: /dev/hda3 是指第一个 IDE 硬盘上的第三个主分区或扩展分区; /dev/sdb6 是第二个 SCSI 硬盘上的第二个逻辑分区。		

① 块设备文件：块设备的主要特点是可以随机读写，而最常见的块设备就是磁盘，如 /dev/hda1、/dev/sda2、/dev/fd0 等。

② 字符设备文件：同块设备一样，一般都可以用 service kudzu start 命令来自动增加、删除或修改字符设备。最常见的字符设备是打印机和终端，它们可以接收字符流。/dev/null 是一个非常实用的字符设备文件，如果将程序的输出结果重定向到/dev/null，则看不到任何输出信息。

常见的 Linux 设备文件如表 10-3 所示。

表 10-3 设备文件分类

文 件	说 明
/dev/ttySn	指串行口 (n=0,1,2,...), n=0: 第一个串行口，鼠标通常接在这里。n=1: 第二个串行口，调制解调器很可能接在这里
/dev/modem	串口调制解调器。通常是一个指向 /dev/ttyS1、/dev/ttyS2 或 /dev/ttyS3 的符号链接，具体取决于调制解调器接在哪个串行端口
/dev/mouse	鼠标。通常是一个指向/dev/ttyS0 或相似设备（见上）的符号链接，具体取决于鼠标接在哪个串行端口
/dev/lpn	指并行口 (n=0,1,2,...), n=0: 接在第一个并行口的打印机，通常打印机接在这里
/dev/fdn	指软驱接口 (n=0,1,2,...), n=0: 第一个软盘驱动器（一般都有）
/dev/hdxn	指硬盘接口 (x=a,b,c,...), x=a: 第一个 IDE 硬盘（整个硬盘）。大多数 IBM 兼容 PC 的硬盘是 IDE 设备。x=b: 第二个 IDE 硬盘（整个硬盘）。在很多计算机中，IDE 光驱接在这里。(n=1,2,3,...), /dev/hda1: 第一个 IDE 硬盘的第一个分区。不难猜测，/dev/hdd8 将会是第四个 IDE 硬盘的第八分区。同理，如/dev/sda: 第一个 SCSI 硬盘（注意 fd, hd, sd 等关键标识）
/dev/cdrom	指向相应设备的链接，通常是/dev/hdc 或/dev/hdb（CD-ROM）或/dev/scd0（CD-R/RW）
/dev/ptyn	n=1,2,3,..., n=1: 第一个字符终端。n=2: 第二个字符终端，以此类推
/dev/dsp	数字音频，dsp 是“Digital Signal Processing（数字信号处理）”，例如声卡

(2) 用户权限

在 Linux 系统中，每一个文件和目录都有相应的访问许可权限，文件或目录的访问权限分为可读（可列目录）、可写（对目录而言是可以在目录中做写操作）和可执行（对目录而言是可以访问的）三种，分别以 r, w, x 表示，其含义为：对于一个文件来说，可以将用户分成三种文件所有者、同组用户、其他用户，可对其分别赋予不同的权限。每一个文件或目录的访问权限都有三组，每组用三位字符表示，如图 10-1 所示。

注：文件类型有多种，d 代表目录，- 代表普通文件，c 代表字符设备文件。

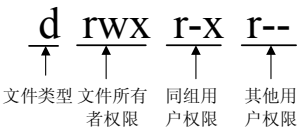


图 10-1 权限位示意图

chmod 的语法格式为：

chmod [who] [opt] [mode] 文件/目录名

其中 who 表示对象，是以下字母中的一个或组合：u（文件所有者）、g（同组用户）、o（其他用户）、a（所有用户）；opt 则代表操作，可以为：+（添加权限）、-（取消权限）、=（赋予给定的权限，并取消原有的权限）；而 mode 则代表权限。

在不考虑 UMASK 的情况下，新建一个文件或目录的权限应该都是 `rw-rw-rw-`，但为了提高安全性，会默认去除新建文件的可执行权限（x）。而对于新建的目录，可执行位 x 与是否被允许进入该目录有关，因此 Linux 约定：

新建文件的权属是 `-rw-rw-rw-`，权限值是 666。

新建目录的权属是 `drwxrwxrwx`，权限值是 777。

那么，在给定系统 UMASK 的情况下，新建文件或目录的默认权限如下赋予：

新建文件的约定权限-UMASK 表示的权限=文件的默认权限

新建目录的约定权限-UMASK 表示的权限=目录的默认权限

这里的减号（-），更确切地说是屏蔽的意思。

一般系统的 UMASK 默认值为 022，或者表示为 `--- -w- -w-`。那么新建一个文件或目录的默认权限为：

新建文件的约定权限-UMASK 表示的权限=文件的默认权限

$(-rw-rw-rw-) - (--- -w- -w-) = (-rw-r-r-)$

注：所谓数字表示法是指将读取（r）、写入（w）和执行（x）分别以 4、2、1 来代表，没有授予的部分就表示值为 0，然后再把所授予的权限相加而成。

（3）基本操作命令

Linux 的系统结构可以分为三层：最内层是系统核心，中间层是 Shell（壳）、库函数，最外层是应用程序。Linux 的常用命令如表 10-4 所示。

表 10-4 Linux 的常用命令

命 令	命 令 说 明	等价的 DOS 命令
pwd	显示当前工作目录和路径名	不带参数的 cd 命令
ls	列出目录内容	dir 命令
cp	复制文件内容，可复制整个目录	copy 命令
cat	串接并显示文件，可同时显示多个文件	type 命令
cd	改变当前工作目录	cd 命令
rm	删除文件和目录	del 和 rmdir 命令
mv	移动文件	move 命令
ps	显示当前进程	无对应
kill	中止某个进程	无对应
chmod	设置文件、目录的权限	无对应

另外，tar 命令在往年考试中也有考查，该命令具体介绍如下。

格式：tar 选项文件目录列表

功能：对文件目录进行打包备份。

选项：

-c, 建立新的归档文件;
-r, 向归档文件末尾追加文件;
-x, 从归档文件中解出文件;
-O, 将文件解开到标准输出;
-v, 处理过程中输出相关信息;
-f, 对普通文件操作;
-z, 调用 `gzip` 来压缩归档文件, 与-x 联用时调用 `gzip` 完成解压缩;
-Z, 调用 `compress` 来压缩归档文件, 与-x 联用时调用 `compress` 完成解压缩。

例如, 将当前目录下所有.txt 文件打包并压缩归档到文件 `this.tar.gz` 中, 可以使用:

```
tar czvf this.tar.gz ./*.txt
```

将当前目录下的 `this.tar.gz` 中的文件解压到当前目录中, 可以使用:

```
tar xzvf this.tar.gz ./
```

Linux 的三种进程查看命令介绍如下。

① who 命令

该命令主要用于查看当前在线上的用户情况。如果用户想和其他用户建立即时通信, 如使用 `talk` 命令, 那么首先要确定的就是该用户确实在线上, 不然 `talk` 进程就无法建立起来。又如, 系统管理员希望监视每个登录的用户此时此刻的所作所为, 也要使用 `who` 命令。

语法格式如下:

```
who [imgsuwHT] [--count] [--idle] [--heading] [--help] [--message] [--mesg]
[--version] [--writable] [file] [am i]
```

所有的选项都是可选的, 也就是说, 可以单独使用 `who` 命令。不使用任何选项时, `who` 命令将显示以下三項内容。

login name: 登录用户名;

terminal line: 使用终端设备;

login time: 登录到系统的时间。

如果给出的是两个非选项参数, 那么 `who` 命令将只显示运行 `who` 程序的用户名、登录终端和登录时间。通常这两个参数是 “`am i`”, 即该命令格式为 “`who am i`”。

下面对 `who` 命令的常用参数进行说明。

-m, 和 “`who am i`” 的作用一样, 显示运行该程序的用户名。

-q, --count, 只显示用户的登录账号和登录用户的数量, 该选项优先级高于其他任何选项。

-s, 忽略。主要是用于和其他版本的 `who` 命令兼容。

-i, -u, --idle, 在登录时间后面显示该用户最后一次对系统进行操作至今的时间, 也就是常说的 “发呆” 时间。

② w 命令

该命令也用于显示登录到系统的用户情况, 但是与 `who` 不同的是, `w` 命令功能更加强大, 它不但可以显示有谁登录到系统, 还可以显示出这些用户当前正在进行的工作, 并且统

计的数据相对 **who** 命令来说更加详细和科学,可以认为 **w** 命令就是 **who** 命令的一个增强版。

w 命令的显示项目按以下顺序排列:当前时间,系统启动到现在的时间,登录用户的数目,系统在最近 1 秒、5 秒和 15 秒的平均负载。然后是每个用户的各项数据,项目显示顺序如下:登录账号、终端名称、远程主机名、登录时间、空闲时间、JCPU、PCPU、当前正在运行进程的命令行。

其中,JCPU 时间指的是和该终端(tty)连接的所有进程占用的时间。这个时间里并不包括过去的后台作业时间,但包括当前正在运行的后台作业所占用的时间。而 PCPU 时间则是指当前进程(即在 **what** 项中显示的进程)所占用的时间。下面介绍该命令的具体用法和参数。

语法格式如下:

```
w [-husfV] [user]
```

下面对参数进行说明。

-h, 不显示标题。

-u, 当列出当前进程和 CPU 时间时忽略用户名。主要用于执行 **su** 命令后的情况。

-s, 使用短模式。不显示登录时间、JCPU 和 PCPU 时间。

-f, 切换显示 **FROM** 项,也就是远程主机名项。默认值是不显示远程主机名的,当然系统管理员可以对源文件做一些修改,使得显示该项成为默认值。

-V, 显示版本信息。

user, 只显示指定用户的相关情况。

③ ps 命令

要对进程进行监测和控制,首先必须要了解当前进程的情况,也就是需要查看当前进程,而 **ps** 命令就是最基本也是非常强大的进程查看命令。使用该命令可以确定有哪些进程正在运行和运行的状态、进程是否结束、进程有没有僵死、哪些进程占用了过多的资源等。总之,大部分信息都是可以通过执行该命令得到的。

语法格式如下:

```
ps [选项]
```

下面对命令选项进行说明。

-e, 显示所有进程。

-f, 全格式。

-h, 不显示标题。

-l, 长格式。

-w, 宽输出。

A, 显示终端上的所有进程,包括其他用户的进程。

R, 只显示正在运行的进程。

X, 显示没有控制终端的进程。

该命令显示的相关字段解释如下。

uptime, 该项显示的是系统启动时间、已经运行的时间和三个平均负载值(最近 1 秒、

5 秒、15 秒的负载值)。

Processes，自最近一次刷新以来的运行进程总数。当然这些进程被分为正在运行的、休眠的、停止的等很多种类。进程和状态显示可以通过交互命令 **t** 来实现。

CPU states，显示用户模式、系统模式、优先级进程（只有优先级为负的列入考虑）和闲置等各种情况所占用 CPU 时间的百分比。优先级进程所消耗的时间也被列入到用户和系统的时间中，所以总的百分比将大于 100%。

Mem，内存使用情况统计，其中包括总的可用内存、空闲内存、已用内存、共享内存和缓存所占内存的情况。

Swap，交换空间统计，其中包括总的交换空间、可用交换空间和已用交换空间。

PID，每个进程的 ID。

PPID，每个进程的父进程 ID。

UID，每个进程所有者的 UID。

USER，每个进程所有者的用户名。

PRI，每个进程的优先级别。

NI，该进程的优先级值。

SIZE，指该进程的代码大小、数据大小以及堆栈空间大小的总数。其单位是 KB。

TSIZE，该进程的代码大小。对于内核进程这是一个很奇怪的值。

DSIZE，数据和堆栈的大小。

TRS，文本驻留大小。

D，被标记为“不干净”的页项目。

LIB，使用库页的大小。对于 ELF 进程没有作用。

RSS，该进程占用的物理内存的总数量，其单位是 KB。

SHARE，该进程使用共享内存的数量。

STAT，该进程的状态。其中：

S 代表休眠状态；

D 代表不可中断的休眠状态；

R 代表运行状态；

Z 代表僵死状态；

T 代表停止或跟踪状态。

TIME，该进程自启动以来所占用的总 CPU 时间。

3. 网络基本参数配置

本考点主要考查在 Linux 下基本网络参数具体配置方法，而 Windows 下的基本网络参数配置相对简单，界面通俗易懂，这里就不再介绍了。

(1) 网络配置命令

常用的网络配置命令及含义如下。

① **netconf**：图形化的网络参数配置命令。

② **ifconfig**: 是 Linux 系统中最常用的一个用来显示和设置网络设备的工具。以下是一些常用的命令组合。

将第一块网卡的 IP 地址设置为 192.168.0.1:

```
ifconfig eth0 192.168.0.1
```

格式: **ifconfig** 网络设备名 IP 地址。

暂时关闭或启用网卡:

关闭第一块网卡——**ifconfig eth0 down**。

启用第一块网卡——**ifconfig eth0 up**。

将第二块网卡的子网掩码设置为 255.255.255.0:

```
ifconfig eth1 netmask 255.255.255.0
```

格式: **ifconfig** 网络设备名 **netmask** 子网掩码。

我们也可以同时设置 IP 地址和子网掩码:

```
ifconfig eth1 192.168.0.1 netmask 255.255.255.0
```

将第一块网卡的广播地址设置为 192.168.0.255:

```
ifconfig eth0 -broadcast 192.168.0.255
```

③ **route**: 用来查看和设置 Linux 系统的路由信息, 以实现与其他网络的通信。

增加一个默认路由: **route add 0.0.0.0 gw** 网关地址。

删除一个默认路由: **route del 0.0.0.0 gw** 网关地址。

指定一个路由: **route add** 目标网络 **gw** 网关地址。

④ **ping**: 与 Windows 下的 **ping** 命令类似, 在此不再详述。

⑤ **tracert**: 与 Windows 下的 **tracert** 命令类似, 在此不再详述。

⑥ **netstat**: 功能十分强大的查看网络状态的工具。

统计出各网络设备传送、接收数据报的情况: **netstat -i**。在该命令输出的项目中将包括如表 10-5 所示的信息。

表 10-5 netstat 输出项目

表 项	说 明	表 项	说 明
Iface	网络接口名	MTU	最大传输单元
RX-OK	成功接收包总数	RX-ERR	接收的错误包总数
RX-DRP	接收时丢包总数	RX-OVR	接收的碰撞包总数
TX-OK	成功发送包总数	TX-ERR	发送的错误包总数
TX-DRP	发送时丢包总数	TX-OVR	发送的碰撞包总数

显示网络的统计信息: **netstat -s**。将以摘要的形式统计出 IP、ICMP、TCP、UDP、TCPEXT 形式的通信信息。

显示出 TCP 传输协议的网络连接情况: **netstat -t**, 将列出每个连接的状态, 包括本地 IP 地址、远端 IP 地址、连接状态。

只显示出使用 UDP 的网络连接情况: **netstat -t**。

显示路由表: **netstat -r**, 输出内容与 **route** 相同。

(2) 常用的网络配置文件

常用的网络配置文件如表 10-6 所示。

表 10-6 常用的网络配置文件

文 件 名	功 能
/etc/hosts	存放的是一组 IP 地址与主机名的列表，对其进行域名解析
/etc/hosts.conf	指定域名解析方法的顺序，如 order hosts, dns, 先用/etc/hosts, 再用 DNS
/etc/resolv.conf	存放域名服务器的 IP 地址
/etc/protocols	存放协议和协议号之间的映射关系
/etc/services	用于定义现有的网络服务

(3) 部分配置文件解析

① DNS 客户端配置文件

```
[root@localhost etc]# cat /etc/resolv.conf
nameserver 210.36.16.33
nameserver 202.103.224.68
search localdomain
```

② IP 配置文件

```
[root@localhost etc]# cat /etc/sysconfig/network-scripts/ifcfg-eth0
DEVICE=eth0
BOOTPROTO=static
HWADDR=00:04:23:C4:9D:0C
IPADDR=192.168.2.86
NETMASK=255.255.255.0
ONBOOT=yes
TYPE=Ethernet
```

③ 网关

```
[root@localhost etc]# cat /etc/sysconfig/network
NETWORKING=yes
HOSTNAME=localhost.localdomain //命令行显示的名字，如[root@localhost ~]#
GATEWAY=192.168.2.254 //也可以放在 ifcfg-eth0
```

④ 主机名

```
[root@localhost patches]# cat /etc/hosts
# Do not remove the following line, or various programs
# that require network functionality will fail.
127.0.0.1 localhost.localdomain localhost
```

10.2.2 一点一练

试题 1

在一台 256MB RAM 的计算机上安装 Linux 系统，交换分区（Swap）的大小合理的设置应该为____(1)_____。

- (1) A. 128MB B. 512MB C. 1024MB D. 4096MB

试题 2

在 Linux 中系统的配置文件存放在____(2)_____目录下。

- (2) A. /bin B. /etc C. /dev D. /root

试题 3

在 Linux 中, 下列____(3)____可以获得任何 Linux 命令的在线帮助。

- (3) A. #help <command> B. #show <command>
C. #man <command> D. #ls <command>

试题 4

在 Linux 中, ____ (4) ____ 命令可用显示当前用户的工作目录。

- (4) A. #where B. #md C. #pwd D. #rd

试题 5

下列选项中, ____ (5) ____ 不属于 Windows 的网络应用程序接口 (API)。

- (5) A. Winsock B. NFS C. RPC D. NetBIOS

试题 6

在 Linux 操作系统中把外部设备当作文件统一管理, 外部设备文件通常放在____(6)____目录中。

- (6) A. /dev B. /lib C. /etc D. /bin

试题 7

下列____(7)____命令可以更改一个文件的权限设置。

- (7) A. attrib B. file C. chmod D. change

试题 8

在 Windows 网络操作系统通过域模型实现网络安全管理策略。下列除____(8)____以外都是基于域的网络模型。在一个域模型中不允许包含____(9)____。

- (8) A. 单域模型 B. 主域模型 C. 从域模型 D. 多主域模型
(9) A. 多个主域控制器 B. 多个备份域控制器
C. 多个主域 D. 多个服务器

试题 9

在 Linux 操作系统中, 命令“chmod -777/home/abc”的作用是____(10)____。

- (10) A. 把所有的文件复制到公共目录 abc 中
B. 修改 abc 目录的访问权限为可读、可写、可执行
C. 设置用户的初始目录为/home/abc
D. 修改 abc 目录的访问权限为对所有用户只读

试题 10

若在 Windows “运行”窗口中键入____(11)____命令, 则可运行 Microsoft 管理控制台。

- (11) A. CMD B. MMC C. AUTOEXE D. TTY

10.2.3 解析与答案

试题 1 分析

交换分区 (Swap) 的合理值一般在内存的两倍左右, 可以适当加大。

试题 1 答案

- (1) B

试题 2 分析

Linux 各文件夹的作用如下。

/bin: 二进制可执行命令。
/dev: 设备特殊文件。
/etc: 系统管理和配置文件。
/etc/rc.d: 启动的配置文件和脚本。
/home: 用户主目录的基点, 比如用户 user 的主目录就是/home/user, 可以用~user 表示。
/lib: 标准程序设计库, 又叫动态链接共享库, 作用类似 Windows 里的.dll 文件。
/sbin: 统管理命令, 这里存放的是系统管理员使用的管理程序。
/tmp: 公用的临时文件存储点。
/root: 系统管理员的主目录 (特权阶级)。
/mnt: 系统提供这个目录是让用户临时挂载其他的文件系统。
/lost+found: 这个目录平时是空的, 是系统非正常关机时而留下“无家可归”的文件。
/proc: 虚拟的目录, 是系统内存的映射。可直接访问这个目录来获取系统信息。
/var: 某些大文件的溢出区, 例如各种服务的日志文件。
/usr: 最庞大的目录, 要用到的应用程序和文件几乎都在这个目录。其中包含如下文件夹。
 /usr/x11r6: 存放 x window 的目录。
 /usr/bin: 众多的应用程序。
 /usr/sbin: 超级用户的一些管理程序。
 /usr/doc: Linux 文档。
 /usr/include: Linux 下开发和编译应用程序所需要的头文件。
 /usr/lib: 常用的动态链接库和软件包的配置文件。
 /usr/man: 帮助文档。
 /usr/src: 源代码, Linux 内核的源代码就放在/usr/src/linux 里。
 /usr/local/bin: 本地增加的命令。
 /usr/local/lib: 本地增加的库。

试题 2 答案

(2) B

试题 3 分析

Linux 系统下获取命令在线帮助信息的方法是运行 man 和 info 的方法, 分别可以看到查询关键命令字的手册页与信息页内容。

试题 3 答案

(3) C

试题 4 分析

在 Linux 中, 是用 pwd 命令显示当前用户的工作目录。pwd 命令的功能是显示用户当前所处的目录, 该命令显示整个路径名, 并且显示当前工作目录的绝对路径。在 Linux 中创建一个新目录的命令是 mkdir, 类似 DOS 下的 md 命令; 删除一个目录的命令是 rmdir, 类似 DOS 下的 rd 命令。

试题 4 答案

(4) C

试题 5 分析

Windows 系统除了实现操作系统的各种管理功能之外, 同时还提供了面向用户的系统服务应用程序接口, 通常称为程序接口 (Application Programming Interface), 简称 API 函数。

这些函数是 Windows 提供给应用程序与操作系统的接口、在程序中通过 API 函数调用，可以实现各种界面丰富、功能灵活的应用程序。所以可以认为 API 函数是构筑整个 Windows 框架的基础，在它的下面是 Windows 的操作系统核心，而它的上面则是 Windows 丰富多彩和功能强大的应用程序。其中 Winsock 是 Windows Sockets 的缩写，它作为 Windows 和 TCP/IP 之间的接口，是在网络编程中使用最广泛的应用编程接口。

RPC (Remote Procedure Calls) 是远程过程调用协议，可以由用户程序使用向网络中的另一台计算机上的程序请求服务。由于使用 RPC 的程序不必了解支持通信的网络协议的情况，因此 RPC 提高了程序的互操作性。在 RPC 中，发出请求的程序是客户程序，而提供服务的程序是服务器，RPC (远程过程调用) 是一项广泛用于支持分布式应用程序 (不同组件分布在不同计算机上的应用程序) 的级数。RPC 的主要目的是为组件提供一种相互通信的方式，使这些组件之间能够互相发出请求并传递这些请求的结果。

NetBIOS (Network Basic Input/Output System) 网络基本输入/输出系统是 1983 年 IBM 开发的一套网络协议标准。微软的客户机/服务器模式的网络通信系统就是基于 NetBIOS 协议的。应用程序通过标准的 NetBIOS API 调用，实现 NetBIOS 命令和数据在各种协议中传输。

而 NFS (Network File System) 是网络文件系统，最早是由 SUN 公司所发展出来的，NFS 的主要功能是通过网络使不同的计算机和不同的操作系统之间实现文件共享。

试题 5 答案

(5) B

试题 6 分析

本题考查 Linux 中有关文件系统与设备文件管理的概念和知识。

在 Linux 系统中，把每一种 I/O 设备都映射成为一个设备文件，可以像普通文件一样处理，这就使得文件与设备的操作尽可能统一。外部设备文件分为字符设备文件和块设备文件，对应于字符设备和块设备。Linux 把对设备的 I/O 作为普通文件的读取/写入，操作内核提供了对设备处理和对文件处理的统一接口。每一种 I/O 设备对应一个设备文件，存放在/dev 目录中，如行式打印机对应/dev/lp，第一个软盘驱动器：/dev/fd0 等。

试题 6 答案

(6) A

试题 7 分析

本题测试 Linux 操作系统中有关文件访问权限管理命令的概念和知识。

Linux 对文件的访问设定了 3 级权限；文件所有者、同组用户和其他用户。对文件的访问设定了 3 种处理操作：读取、写入和执行。改变文件或目录访问权限 chmod 命令用于改变文件或目录的访问权限，这是 Linux 系统管理员最常用到的命令之一。在默认情况下，系统将新创建的普通文件的权限设置为 -rw-r-r-，将每一个用户所有者目录的权限都设置为 drwx-----。根据需要可以通过命令修改文件和目录的默认存取权限。只有文件所有者或超级用户 root 才有权使用 chfmod 改变文件或目录的访问权限。

试题 7 答案

(7) C

试题 8 分析

本题考查 Windows 网络操作系统中有关域模型管理方面的概念和知识。

Windows 域也称之为域模型，是 Windows 系统中实现网络管理与安全策略的独立运行

单位，一个域可以包含一个或多个 Server 及工作站。域之间不但可以按需要相互进行管理，还可以跨网分配文件和打印机等设备资源，使不同的域之间实现网络资源的共享与管理。域模型主要分为单域模型、主域模型、多主域模型和完全信任模型。

Windows 域是由各种服务器、客户计算机和工作站组成的。其中，主域控制器（Primary Domain Controller，PDC）是一台运行 Windows Server 的服务器，并且该服务器必须是主域控制器 PDC。可以将 PDC 同时作为文件服务器、打印服务器或应用软件服务器使用，但是一个域模型必须有且只有一个 PDC。域中所有用户账号、用户组设置，以及安全设置等数据都保存在 PDC 的目录数据库中，账号的新增与修改都是在 PDC 的目录数据库上。因此，在 Windows 域中，网络主控管理信息（Master Copy）保存在 PDC 上。Windows 网络管理员按照域方式构建 Windows 网络时，域内设立的第一台计算机必须是 PDC。在日常运转中，PDC 负责审核（Authenticate）登录者的身份，判别其是否为合法用户。而备份域控制器（Backup Domain Controller，BDC）可以同时用做文件服务器、打印服务器或应用软件服务器。NT 域中的 PDC 会定期地将其用户与组账号数据复制到 BDC 中。除了 PDC 外，BDC 也负责审核登录者的身份。域内不一定必须有 BDC，但是建议一个域最少有一台 BDC。尤其是大型的网络，需要多台 BDC 分担审核登录者身份的操作负荷。当 PDC 因故障或其他原因无法使用时，可将 BDC 升级为主域控制器，让整个域仍然可以正常运行。

试题 8 答案

(8) C

(9) A

试题 9 分析

chmod 命令用来修改文件的权限。命令“chmod-777 /home/abc”等价于“chmod-111111111/home/abc”其作用是修改 abc 目录的访问权限为对任何用户均为可读、可写、可执行。

试题 9 答案

(10) B

试题 10 分析

运行 Microsoft 管理控制台，必须在 Windows “运行”窗口中输入“MMC”。MMC 是 Microsoft Management Console 的缩写。

试题 10 答案

(11) B

10.3 网管体系和故障诊断

在网管体系和故障诊断这个考点中，主要涉及三个方面的知识，分别是网管体系构成、SNMP 管理协议和网络故障诊断命令配置。

10.3.1 考点精讲

Windows 系统基本管理和 Linux 系统基本管理是分别基于 Windows 和 Linux 操作系统进行一系列的诸如系统管理、磁盘管理、安全管理、网络参数配置管理和日志分析等活动，同时也是网络方向从业人员必备的一项基本技能。

通过前面的描述，网络参数配置管理也属于系统管理的一部分，但由于它又涉及网络互连和具体的参考命令（主要针对 Linux 系统），在这里单独作为一个知识点进行分析。

1. 网络管理体系

本知识点主要让考生掌握网管体系结构、网络管理的定义、OSI 标准所定义的 5 个功能, 以及每个功能所包括的内涵。网络管理是一项复杂的系统工程, 它不仅涉及组成网络的各种网络设备、网络对象, 还涉及管理这些不同网络设备或对象的标准。因此要做好网络管理工作, 就需要有一个完备的网络管理解决方案。

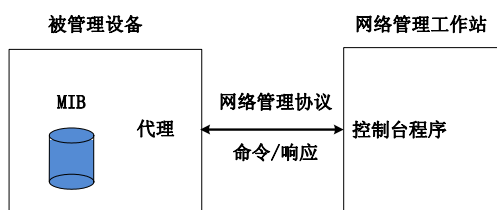


图 10-2 网络管理体系组成图

计算机网络的网络管理系统基本上由五部分组成: 被管设备, 若干被管代理, 至少一个网络管理器, 一种公共网络管理协议, 一种或多种管理信息库(MIB)。网络管理体系结构如图 10-2 所示。

其中被管理设备上的代理是一个程序, 所以, 只要是运行这样的程序, 就可以被视为是一个被管设备, 被管理设备既可以是网络上的路由器、交换机, 也可以是网络上的服务器(但通常不将普通的工作站纳入到被管理设备中)。

MIB 是管理信息库, 网络管理工作站是通过查询这个库来获取设备的信息。

被管理代理与网络管理进程之间的信息交互的动作规则、数据格式等由网络管理协议来规定。网络管理协议与管理信息库一起协调工作简化了网络管理的复杂过程。因为管理信息库的管理信息描述了所有被管理对象及其属性值, 使得网络管理的全部工作就是对这些对象及属性值变量的读取(Get 对应于监视)或设置(Set 对应于控制)。

根据 OSI 网络管理标准, 网络管理包括配置管理、故障管理、性能管理、安全管理及计费管理 5 大功能。

(1) 配置管理: 包括配置信息的自动获取(包括 MIB 中定义的配置信息, 网管标准中未定义但对设备重要、用于管理的辅助信息), 自动配置、备份, 配置一致性检查(路由器端口、路由信息的设置), 用户操作记录功能(即操作日志)。

(2) 故障管理: 包括故障监测、故障报警、故障信息管理、排错支持工具、检索/分析故障信息。

(3) 性能管理: 包括性能监控(由用户定义被管理对象及其属性)、阈值控制(对特定对象的特定属性设置阈值)、性能分析、可视化的性能报告、实时性能监控、网络对象性能查询。

(4) 安全管理: 包括网络管理本身的安全, 以及被管理对象的安全。

网络管理本身安全机制: 管理员身份认证(公钥认证, 局域网内的信任用户, 可用简单口令认证)、管理信息存储和传输的加密与完整性(SSL、加密、消息摘要)、网络管理用户分组管理与访问控制、系统日志分析。

网络对象的安全机制: 网络资源的访问控制(访问控制链表)、报警事件分析(发现可疑的攻击迹象)、主机系统的安全漏洞检测。

(5) 计费管理: 包括计费数据采集、数据管理与数据维护、计费政策制定、政策比较与决策支持、数据分析与费用计算、数据查询。

在历年考试题中, 经常出现指出 5 大功能项中的细节内容, 要求考生指出对应的功能项。考生在记忆时应重在理解, 找到联系: 配置管理主要在于网络管理的信息配置方面; 故障管理主要在于故障发现、报警方面; 性能管理主要是监控一些关键运行指标; 安全管理主要是安全分析方面; 计费管理主要是对计费信息进行统计。

2. SNMP 管理协议

本知识点重点在于让考生了解 SNMP 协议组的构建、管理模型的构成、各版本的区别、MIB 基础知识，要求掌握 SNMP 的协议基础、特点以及 5 种常见 PDU 的功能与特点。

SNMP 是基于 TCP/IP 协议族的网络管理标准，它的前身是 SGMP（简单网关监控协议）。SNMPv1 是 IETF 在 1990 年发布的，后来又发布了 SNMPv2 和 SNMPv3。SNMP 是一组协议标准，它主要包括管理信息库（MIB）、管理信息结构（SMI）和简单网络管理协议（SNMP）三个部分。其网络管理模型则是由管理进程（Manager，处于管理模型核心，负责完成网管各项功能）、代理（Agent，运行在设备上的管理程序，负责收集信息）和管理信息库三个部分组成的。

（1）SNMP 协议和版本区别

① SNMPv1：由于轮询的性能限制，SNMP 不适合管理很大的网络，不适合检索大量数据。SNMP 的陷入报文是没有应答的，可能会丢掉重要的管理信息。SNMP 只提供简单的团体名认证，安全措施很弱。SNMP 不支持管理站之间的通信。

② SNMPv2：管理者与管理者之间可以通信。SNMPv2 提供 3 种访问管理信息的方法，包括管理站和代理之间的在请求/响应通信；代理系统到管理站的非确认通信；管理站和管理站之间的请求/响应通信，以支持分布式网络管理。SNMPv2 报文的结构分为 3 个部分——版本号、团体名和作为数据传送的 PDU。

SNMPv2 访问管理信息的方法如下。

管理站和代理之间的请求/响应通信，与 SNMPv1 是一样的。

管理站和管理站之间的请求/响应通信，是 SNMPv2 特有的。

代理系统到管理站的非确认通信，即由代理向管理站发送陷入报文，通知出现的异常情况。SNMPv1 中也有对应的通信方式。

SNMPv2 实体发送报文的步骤如下。

- a. 根据要实现的协议操作构造 PDU。
- b. 把 PDU、源和目标端口地址以及团体名传送给认证服务，认证服务产生认证码或对数据进行加密，返回结果。
- c. 加入版本号和团体号，构造报文。
- d. 进行 BER 编码，产生 0/1 比特串，发送出去。

SNMPv2 实体接收报文的步骤如下。

- a. 对报文进行语法检查，丢弃出错的报文。
- b. 把 PDU 部分、源和目标端口号交给认证服务。如果认证失败，发送一个陷入报文，丢弃报文。
- c. 如果认证通过，则把 PDU 转换成 ASN.1 的形式。
- d. 协议实体对 PDU 做语法检查，如果通过，根据团体名和适当的访问策略做相应的处理。

③ SNMPv3：提供了数据源标识、报文完整性认证、防止重放、报文机密性、授权和访问控制、远程配置与高层管理。

表 10-7 对这 3 种协议进行了集中比较。

表 10-7 SNMP 协议比较

版 本	特 色	增 强
SNMPv1	简单，易于实现，广泛应用	
SNMPv2	支持完全集中和分布式两种网络管理	扩充了管理信息结构、增强了管理站间的通信能力，添加了新的协议操作
SNMPv3	达到商业级安全要求	提供了数据源标识、报文完整性认证、防止重放、报文机密性、授权和访问控制、远程配置和高层管理

（2）MIB 与 MIB-2

MIB 是网络管理系统中的重要构件，由系统内许多被管理的对象及属性组成。它是一个虚拟的数据库，采用树型结构组织。它经历了 MIB-1 和 MIB-2 两个版本。MIB-2 定义了系统组（System）、接口组（Interface）、地址转换组（Address Translation）、IP 组、ICMP 组、TCP 组、UDP 组、EGP 组、传输组（Transmission）和 SNMP 等 11 个功能组。SNMP 现在使用的是 MIB-2。

（3）SNMP 协议的工作模式

SNMP 使用 UDP 作为传输协议，是一种异步的请求/响应协议，其默认端口有两个：一个是用于数据传送与接收的 161 号端口；另一个是用于报警（Trap）信息接收的 162 号端口。

SNMPv1 使用了 5 种格式的 PDU（协议数据单元），也是 SNMP 系列协议中最基础的部分。

① Get-Request：由管理进程发送，向管理代理请求它们的取值。

② Get-NextRequest：由管理进程发送，在 Get-Request 报文后使用，表示查询 MIB 中的下一个对象，常用于循环查询。

③ Set-Request：由管理进程发出，用来请求改变管理代理上的某些对象。

④ Get-Response：当管理代理收到管理进程发送的 Get-Request 或 Get-NextRequest 报文时，将应答一个该报文。

注：以上 4 种均为简单的请求/响应机制，前三种都是原子操作。

⑤ Trap：是一种报警机制（即属于无请求的），用于在意外或突发故障情况下，管理代理主动向管理进程发送报警信息。常见的报警类型有冷启动、热启动、线路故障、线路故障恢复和认证失败等。

与 SNMPv1 不同的是，SNMPv2 不仅支持管理站（管理进程）与管理代理进行请求/响应通信，还允许管理站之间进行通信。

3. RMON 及其他协议

RMON（远程网络监控协议）也是一种监控局域网通信的标准。它在 SNMP 管理信息库的基础上进行了扩充，能够实现离线操作、主动监视、问题检测和报告、提供增值数据、多管理站操作等。RMON 的目标是为了扩展 SNMP 的 MIB-2（管理信息库），使 SNMP 更为有效、更为积极主动地监控远程设备。RMON MIB 由一组统计数据、分析数据和诊断数据构成，利用许多供应商生产的标准工具都可以显示出这些数据，因而它具有独立于供应商的远程网络分析功能。

RMON 规范的大部分是 RMON 管理信息库（RMON MIB）的定义，这一 MIB 现已被吸收进 MIB-2，其子树标识符是 16。RMON MIB 的结构分为以下 9 组。

① 统计 (Statistics): 维护代理监视的每一个子网的基本使用情况和错误统计。

② 历史 (History): 记录从统计组可以得到的信息的周期性统计样本。

③ 警报 (Alarm): 允许管理控制台人员为 RMON 代理记录的任何记数和整数设置采样间隔和报警阈值。

④ 主机 (Host): 包括关于连接到子网上的主机的各种流量的计数。

⑤ 最高N台主机 (HostTopN): 包含排序后的主机统计信息。

⑥ 矩阵 (Matrix): 以矩阵形式显示出错和使用信息。

⑦ 过滤 (Filter): 允许监视器观测与一个过滤器相匹配的数据报。

⑧ 包捕获 (Packet capture): 控制数据被发往管理控制台的方式。

⑨ 事件 (Event): 一个关于由 RMON 代理产生的所有事件的表。

RMON MIB 中的所有组都是可选的,但它们之间有一些依赖性:警报组需要事件组的实现;最高N台主机 (hostTopN) 组需要主机组的实现;包捕获组需要过滤组的实现。

除了理论标准 CMIS/CMIP 和事实标准 SNMP 外,常见的其他网管协议规范还包括以下几个。

(1) CMOT: 公共管理信息服务与协议,它在 TCP/IP 协议族上实现了 CMIS 服务。它是一个过渡性解决方案,提供给想过渡到 OSI 网络管理协议的用户使用。

(2) LMMP: 局域网个人管理协议,试图为 LAN 环境提供一个网络管理方案,它工作在 LLC 层,不依赖于任何特定的网络协议,它更容易实现,但不能跨越路由器。

(3) TMN: 电信管理网 (M.30 建议),目的是利用既简单又统一的方法来管理各种不同功能的网络。TMN 的最大优势在于其信息模型的标准化,统一多个厂家设备的规范管理;而其最大的不足是处理时延长,不能满足一些实时处理的要求,而且它是工作在网元级的,没有站在全网的基础上建模。近年来,其最新的发展是使用 CORBA 技术来完善 TMN。

(4) 基于 CORBA 的网络管理: 2000 年版的 M.3010 和 M.3013 为 CORBA 技术引入到以 TMN 为基础的网络管理框架中铺平了道路; X.780 和 Q.816 分别规定了采用细粒度方法的基于 CORBA 技术的网络管理接口定义指南和所需的 CORBA 服务; X.780.1 和 Q.816.1 分别规定了采用粗粒度方法的基于 CORBA 技术的网络管理接口定义指南和所需的 CORBA 服务。

4. 网络故障诊断

此知识点主要包括 Windows/Linux 操作系统下网络故障的诊断及相应的诊断命令的使用。

(1) Windows 网络诊断命令

① winipcfg 命令: Windows 下的 IP 地址配置命令。

② ipconfig 命令: 用于显示 TCP/IP 配置,以下是一些常见的命令选项。

ipconfig/all: 显示所有配置信息。

ipconfig/release: 释放 IP 地址。

ipconfig/renew: 重新获得一个 IP 地址,会向 DHCP 服务器发出新请求。

ipconfig/flushdns: 清空 DNS 解析器缓存。

ipconfig/registerdns: 更新所有 DHCP 租约并重新注册 DNS 域名。

ipconfig/displaydns: 显示 DNS 解析器缓存。

ipconfig/setclassid: 设置 DHCP 类 ID。

③ **ping** 命令: 基于 ICMP 协议, 用于把一个测试数据报发送到规定的地址, 如果一切正常则返回成功响应。它常用于以下几种情形。

验证 TCP/IP 协议是否正常安装: **ping 127.0.0.1**, 如果正常返回, 说明安装成功。其中 127.0.0.1 是回送地址。

验证 IP 地址配置是否正常: **ping** 本机 IP 地址。

查验远程主机: **ping** 远端主机 IP 地址。

④ **nbtstat:** 用于显示 NetBIOS 协议的统计信息, 以及 NetBIOS 地址与 IP 地址的对应关系。

⑤ **netstat:** 网络状态查看命令, 以下是一些常见的命令选项。

netstat -a: 显示所有连接和监听端口。

netstat -e: 显示以太网统计信息。

netstat -n: 以数字格式显示 IP 地址。

netstat -o: 显示每个连接所属的处理 ID。

netstat -p: 显示特定协议的连接。

netstat -r: 显示路由表。

netstat -s: 显示每个协议统计。

⑥ **tracert:** 用于查看分组传链路路径。

(2) Linux 网络诊断命令

下面介绍在 Linux 系统中, 常用的网络诊断命令及格式。

① **ifconfig:** 用于查看和更改网络接口的地址和参数, 包括 IP 地址、网络掩码、广播地址, 使用权限是超级用户。

格式如下:

```
ifconfig -interface [options] address
```

主要参数介绍如下。

-interface: 指定的网络接口名, 如 **eth0** 和 **eth1**。

up: 激活指定的网络接口卡。

down: 关闭指定的网络接口。

broadcast address: 设置接口的广播地址。

pointopoint: 启用点对点方式。

address: 设置指定接口设备的 IP 地址。

netmask address: 设置接口的子网掩码。

② **ping:** 检测主机网络接口状态, 使用权限是所有用户。

格式如下:

```
ping [-dfnqrRv] [-c] [-i] [-I] [-l] [-p] [-s] [-t] IP 地址
```

主要参数介绍如下。

- d: 使用 Socket 的 SO_DEBUG 功能。
- c: 设置完成要求回应的次数。
- f: 极限检测。
- i: 指定收发信息的间隔秒数。
- I: 使用指定的网络界面送出数据报。
- l: 前置载入, 设置在发送出要求信息之前, 先行发出的数据报。
- n: 只输出数值。
- p: 设置填满数据报的范本样式。
- q: 不显示指令执行过程, 开头和结尾的相关信息除外。
- r: 忽略普通的 Routing Table, 直接将数据报发送到远端主机上。
- R: 记录路由过程。
- s: 设置数据报的大小。
- t: 设置存活数值 TTL 的大小。
- v: 详细显示指令的执行过程。

③ netstat: 用于检查整个 Linux 网络状态。

格式如下:

```
netstat [-acCeFghilMnNoprstuvVwx] [-A] [--ip]
```

主要参数介绍如下。

- a (all): 显示所有连线中的 Socket。
- A: 列出该网络类型连线中的 IP 相关地址和网络类型。
- c (continuous): 持续列出网络状态。
- C (cache): 显示路由器配置的快取信息。
- e (extend): 显示网络其他相关信息。
- F (fib): 显示 FIB。
- g (groups): 显示多重广播功能群组组员名单。
- h (help): 在线帮助。
- i (interfaces): 显示网络界面信息表单。
- l (listening): 显示监控中的服务器的 Socket。
- M (masquerade): 显示伪装的网络连线。
- n (numeric): 直接使用 IP 地址, 而不通过域名服务器。
- N (netlink-symbolic): 显示网络外围设备的符号、连接名称。
- o (timers): 显示计时器。
- p (programs): 显示正在使用 Socket 的程序识别码和程序名称。
- r (route): 显示 Routing Table。
- s (statistic): 显示网络工作信息统计表。

- t (tcp): 显示 TCP 传输协议的连线状况。
- u (udp): 显示 UDP 传输协议的连线状况。
- v (verbose): 显示指令执行过程。
- V (version): 显示版本信息。
- w (raw): 显示 RAW 传输协议的连线状况。
- x (unix): 与指定“-A unix”参数相同。
- ip (inet): 与指定“-A inet”参数相同。

④ telnet: 表示开启终端机阶段作业, 并登入远端主机。telnet 是一个 Linux 命令, 同时也是一个协议 (远程登录协议)。

格式如下:

```
telnet [-8acdEfFKLrx] [-b] [-e] [-k] [-l] [-n] [-S] [-X] [主机名称 IP 地址<通信端口>]
```

主要参数介绍如下。

- 8: 允许使用 8 位字符资料, 包括输入与输出。
- a: 尝试自动登录远端系统。
- b: 使用别名指定远端主机名称。
- c: 不读取用户专属目录里的.telnetrc 文件。
- d: 启动排错模式。
- e: 设置脱离字符。
- E: 滤除脱离字符。
- f: 此参数的效果和指定“-F”参数相同。
- F: 使用 Kerberos V5 认证时, 加上此参数可把本地主机的认证数据上传到远端主机。
- k: 使用 Kerberos 认证时, 加上此参数让远端主机采用指定的领域名, 而非该主机的域名。
- K: 不自动登录远端主机。
- l: 指定要登录远端主机的用户名称。
- L: 允许输出 8 位字符资料。
- n: 指定文件记录相关信息。
- r: 使用类似 rlogin 指令的用户界面。
- S: 服务类型, 设置 telnet 连线所需的 IP TOS 信息。
- x: 假设主机有支持数据加密的功能, 就使用它。
- X: 关闭指定的认证形态。

⑤ route: 表示手工产生、修改和查看路由表。

格式如下:

```
# route [-add] [-net|-host] targetaddress [-netmask Nm] [dev] If]
# route [-delete] [-net|-host] targetaddress [gw Gw] [-netmask Nm] [dev] If]
```

主要参数介绍如下。

-add: 增加路由。
-delete: 删除路由。
-net: 路由到达的是一个网络,而不是一台主机。
-host: 路由到达的是一台主机。
-netmask Nm: 指定路由的子网掩码。
gw: 指定路由的网关。
[dev]If: 强迫路由链指定接口。

⑥ nslookup: 查询一台机器的 IP 地址和其对应的域名。使用权限是所有用户。它通常需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器,就可以用这个命令查看不同主机的 IP 地址对应的域名。

格式如下:

```
nslookup [IP 地址/域名]
```

现在网络中已经架设好了一台 DNS 服务器,主机名称为 ns.csai.cn,它可以把域名 http://www.csai.cn 解析为 211.147.214.39 的 IP 地址,这是我们平时用得比较多的正向解析功能。

检测步骤介绍如下。

在 Windows 2000 中选择“开始”→“程序”→“附件”→“命令提示符”选项,在打开的窗口中 C:\>的后面输入 Nslookup www.jsjzx.net,按 Enter 键后即可看到如下结果:

```
Server:ns.csai.cn
Address:211.147.214.30
Name:www.csai.cn
Address:211.147.214.39
```

以上结果显示,正在工作的 DNS 服务器的主机名为 ns.csai.cn,它的 IP 地址是 211.147.214.30,而域名 www.csai.cn 所对应的 IP 地址为 211.147.214.39。那么,在检测到 DNS 服务器 ns.csai.cn 已经能顺利实现正向解析的情况下,它的反向解析是否正常呢?也就是说,能否把 IP 地址 211.147.214.39 反向解析为域名 www.csai.cn?我们在命令提示符 C:\>的后面输入 Nslookup 211.147.214.39,得到结果如下:

```
Server:ns.csai.cn
Address:211.147.214.30
Name:www.csai.cn
Address:211.147.214.39
```

这说明,DNS 服务器的反向解析功能也正常。

然而,有的时候,我们输入 Nslookup www.csai.cn,却出现如下结果:

```
Server:ns.csai.cn
Address:211.147.214.30
*** ns.csai.cn can't find www.csai.cn:Non-existent domain
```

这种情况说明网络中 DNS 服务器 ns.csai.cn 在工作,却不能实现域名 www.jsjzx.net 的正确解析。此时,要分析 DNS 服务器的配置情况,看 www.csai.cn 这一条域名对应的 IP 地址记录是否已经添加到了 DNS 的数据库中。

还有的时候,我们输入 Nslookup www.csai.cn,会出现如下结果:

```
*** Can't find server name for domain:No response from server
```

```
*** Can't repairpc.nease.net:Non-existent domain
```

这时，说明测试主机在目前的网络中，根本没有找到可以使用的 DNS 服务器。此时，我们要对整个网络的连通性进行全面的检测，并检查 DNS 服务器是否处于正常工作状态，采用逐步排错的方法，找出 DNS 服务不能启动的根源。

nslookup 命令用法介绍如下。

- 查询 A 记录

```
C:\>nslookup www.csai.cn
*** Can't find server name for address 192.168.2.1: Non-existent domain
*** Default servers are not available
Server: UnKnown
Address: 192.168.2.1
Non-authoritative answer:
Name: www.csai.cn
Addresses: 211.147.214.,39 202.101.42.101
```

211.147.214.,39,202.101.42.101 即是 WWW 对应的 IP 地址。

- 查询 MX 记录

```
C:\>nslookup -type = mx csai.cn
*** Can't find server name for address 192.168.2.1: Non-existent domain
*** Default servers are not available
Server: UnKnown
Address: 192.168.2.1
Non-authoritative answer:
csai.cn MX preference = 8, mail exchanger = mail.csai.cn
csai.cn nameserver = ns2.csai.cn
mail.csai.cn internet address = 211.147.214.,39
```

mail.csai.cn 是 csai.cn 对应的 MX 记录。

- 查 CNAME 记录

```
C:\>nslookup -type = cname www.csai.cn
*** Can't find server name for address 192.168.2.1: Non-existent domain
*** Default servers are not available
Server: UnKnown
Address: 192.168.2.1
Non-authoritative answer:
www.csai.cn canonical name = www.edu.csai.cn
```

www.edu.csai.cn 是 www.csai.cn 对应的 CNAME 记录。

- 查询域名服务器

```
C:\>nslookup -type = ns csai.cn
*** Can't find server name for address 192.168.2.1: Non-existent domain
*** Default servers are not available
Server: UnKnown
Address: 192.168.2.1
Non-authoritative answer:
cdnunion.com nameserver = ns2.csai.cn
ns2.csai.cn internet address = 211.147.214.30
```

ns2.csai.cn 是 csai.cn 域名的 DNS 服务器。

10.3.2 一点一练

试题 1

在 Windows 命令窗口输入____(1)____命令来查看 DNS 服务器的 IP。

- (1) A. DNSserver B. Nslookup C. DNSconfig D. DNSip

试题 2

在 Windows 中, ping 命令的 -n 选项表示____(2)_____。

- (2) A. ping 的次数 B. ping 的网络号
C. 用数字形式显示结果 D. 不要重复, 只 ping 一次

试题 3

在 Windows 中, tracert 命令的 -h 选项表示____(3)_____。

- (3) A. 指定主机名 B. 指定最大跳步数
C. 指定到达目标主机的时间 D. 指定源路由

试题 4

使用 traceroute 命令测试网络可以____(4)_____。

- (4) A. 检验链路协议是否运行正常
B. 检验目标网路是否在路由表中
C. 检验应用程序是否正常
D. 显示分组到达目标经过的各个路由器

试题 5

能显示 IP、ICMP、TCP、UDP 统计信息的 Windows 命令是____(5)_____。

- (5) A. netstat -s B. netstat -e C. netstat -r D. netstat -a

试题 6

在 RMON 管理信息系统库中, 矩阵组存储的信息是____(6)_____。

- (6) A. 一对主机之间建立的 TCP 连接数 B. 一对主机之间交换的 IP 分组数
C. 一对主机之间交换的字节数 D. 一对主机之间出现冲突的次数

试题 7

假设有一个局域网, 管理站每 15 分钟轮询被管理设备一次, 一次查询访问需要的时间是 200ms, 则管理站最多可以支持____(7)_____个网络设备。

- (7) A. 400 B. 4000 C. 4500 D. 5000

试题 8

在 RMON 中, 实现捕获组 (capture) 时必须实现____(8)_____。

- (8) A. 事件组 (event) B. 过滤组 (filter) C. 警报组 (alarm) D. 主机组 (host)

试题 9

SNMP 和 CMIP 是网络界最主要的网络管理协议, ____ (9) _____是错误的。

- (9) A. SNMP 和 CMIP 采用的检索方式不同
B. SNMP 和 CMIP 信息获取方式不同
C. SNMP 和 CMIP 采用的抽象语法符号不同
D. SNMP 和 CMIP 传输层支持协议不同

试题 10

SNMPv2 引入了信息模块的概念, 用于说明一组定义, 以下不属于这种模块的是____(10)_____。

- (10) A. MIB 模块 B. MIB 的依从性声明模块
C. 管理能力说明模块 D. 代理能力说明模块

10.3.3 解析与答案

试题 1 分析

本题考查 Nslookup 命令。

Nslookup 命令能彻底检查用户的 DNS 服务器。对用户的 DNS 数据库中的每个地址都进行定期逆向解析，以确保所有地址和名字都正确。

Nslookup 命令的使用：Nslookup 是检查我们域名服务器配置的最好工具，它是由 BIND 软件包提供的，它允许任何人直接查询域名服务器，对于确定服务器是否正确地运行和是否配置得合适是很有帮助的。

Nslookup 命令可以交互式地从命令行中进行查询，在命令行中它可以用来查询 IP 地址。

试题 1 答案

(1) B

试题 2 分析

ping 命令的常用参数选项介绍如下。

ping IP -t: 连续对 IP 地址执行 ping 命令，直到被用户按 Ctrl+C 组合键中断。

ping IP -l 2000: 指定 ping 命令中的数据长度为 2000 字节，而不是默认的 32 字节。

ping IP -n: 执行特定次数的 ping 命令。

试题 2 答案

(2) A

试题 3 分析

本题考查 tracert 命令。tracert 命令用于路由的跟踪，加上 -h 选项用于指定最大跳步数。

试题 3 答案

(3) B

试题 4 分析

Linux 的 traceroute 命令可以显示分组到达目标经过的各个路由器的 IP 地址和到达目标的时间，通过 traceroute 可以知道从你的计算机到互联网另一端的主机走的是什么路径。在 MS Windows 中对应的命令为 tracert。

系统管理员在 UNIX 系统中可以直接执行命令 traceroute hostname，在 Windows 系统下执行 tracert hostname。

tracert 命令的其他参数如下介绍。

```
tracert[-d][-h maximum hops][-j computer-list][-w timeout]target_name
```

主要参数介绍如下。

-d: 不对计算机名解析地址。

-h maximum hops: 查找目标的最大跳步数。

-j computer-list: 列出松散源路由。

-w timeout: 等待应答的最大毫秒数。

这类诊断实用程序通过向目标站点发送具有不同生存时间(TTL)的 ICMP 回声(ECHO)报文来确定达到目标的路由。路径上的每个路由器都将 TTL 值减 1，直至 TTL 值减少到 0 时，路由器向源系统发回 ICMP 报时报文。第 1 次发送的 TTL 值为 1，这样可以得到第一个路由器的响应，以后逐渐增加 TTL 的值，就可以得到各个路由器的相应，并测量出达到目标的时间。

试题 4 答案

(4) D

试题 5 分析

netstat 用于显示与 IP、TCP、UDP 和 ICMP 协议有关的统计数据，可以检验本机各端口的网络连接情况。计算机接收到的数据报有时会出错，TCP/IP 容许这类错误，并能够自动进行重发。如果累计的出错数量占到所接收数据报相当大的比例，或者出错数量正在迅速增加，就要用 **netstat** 查一查原因了。

netstat 的常用选项介绍如下。

netstat-s: 分别显示各个协议（IP、ICMP、TCP、UDP）的统计数据。如果应用程序（如 Web 浏览器）运行速度比较慢，或者不能显示 web 页之类的数据，那么可以用本选项来查看一下，确定问题所在。

netstat-e: 用于显示以太网的统计数据，列出的项目包括传送的总字节数、出错数、删除数、数据报的数量和广播的数量。这个选项可以用来统计基本的网络流量。

netstat-r: 显示关于路由表的信息，类似于 **route print** 命令的作用。除了显示有效路由外，还显示当前有效的连接。

netstat-a: 显示所有的有效连接信息列表，包括已建立的连接，也包括监听的连接请求。

netstat-n: 显示所有已建立的有效连接。

试题 5 答案

(5) A

试题 6 分析

矩阵组记录子网中一对主机之间交换的字节数，信息以矩阵的形式储存。矩阵组由 3 个表组成。控制板的一行指明发现主机会话的子网接口。数据表分成源到目标（SD）和目标到源（DS）两个表。如果监视器在某个接口上发现了一对主机会话，则在 SD 表中记录两行，每行表示一个方向的通信。DS 表也包含同样的两行信息，但是索引的顺序不同。这样，管理站可以检索到一个主机向其他主机发送的信息，也可以检索到其他主机向某一个主机发送的信息。

试题 6 答案

(6) C

试题 7 分析

根据题意计算如下：

$$60 \times 15 \times 1000 \div 200 = 4500$$

所以可以轮询 4500 台设备。

试题 7 答案

(7) C

试题 8 分析

RMON 定义的 MIB 是 MIB 下的 16 个子树，共分为 10 组。存储在每一组的信息都是监视器从一个或几个子网中统计和收集的数据。10 组功能是任选的。但实现时有下列连带关系。

- ① 实现警报组时必须实现事件组。
- ② 实现最高 N 台主机时必须实现主机组。
- ③ 实现捕获组时必须实现过滤组。

试题 8 答案

(8) B

试题 9 分析

SNMP 和 GMIP 是最主要的两种网络管理协议。总的来说, SNMP 和 CMIP 两种协议是同大于异。两者的管理目标、基本组成部分都基本相同。在 MIB 库的结构方面, 很多厂商将 SNMP 的 MIB 扩展成与 CMIP 的 MIB 结构相类似, 而且两种协议的定义都采用相同的抽象语法符号 (ASN.1)。

它们的不同之处是, 首先, SNMP 面向单项信息检索, 而 GMIP 则面向组合项信息检索。其次, 在信息获得方面, SNMP 主要基于轮询方式, 而 CMIP 主要采用报告方式。再次, 在传送层支持方面, SNMP 基于无连接的 UDP, 而 CMIP 采用有连接的数据传送。此外, 两者在功能、协议规模、性能、标准化、产品化方面还有相当多的不同点。

试题 9 答案

(9) C

试题 10 分析

SNMPv2 引入了信息模块的概念, 用于说明一组关联的定义。它有 3 种类型的管理信息结构信息模块: MIB 模块、MIB 的依从性声明模块和代理能力说明模块。MIB 模块包含相关的被管理对象的定义。MIB 的依从性声明模块提供描述一组被管理对象的一种系统方法, 必须实现与标准一致。代理能力说明模块显示支持的精确层次, 代理要求考虑 MIB 组。为了代理依照性能声明关联到每个代理, 网络管理系统可以调整它的行为。

试题 10 答案

(10) C

10.4 网管工具与网络存储

在网管工具与网络存储这个考点中, 主要涉及三个方面的知识, 分别是 Sniffer 软件、RAID 和网络存储体系配置。

10.4.1 考点精讲

Sniffer, 中文翻译为嗅探器, 是一种基于被动侦听原理的网络分析方式。使用这种技术方式, 可以监视网络的状态、数据流动情况以及网络上传输的信息。

磁盘阵列 (Redundant Arrays of Inexpensive Disks, RAID), 有“价格便宜具有冗余能力的磁盘阵列”之意。其原理是利用数组方式来做磁盘组, 配合数据分散排列的设计, 提升数据的安全性。磁盘阵列是由很多价格较便宜的磁盘, 组合成一个容量巨大的磁盘组, 利用个别磁盘提供数据所产生加成效果提升整个磁盘系统效能。利用这项技术, 将数据切割成许多区段, 分别存放在各个硬盘上。磁盘阵列还能利用同位检查 (Parity Check) 的观念, 在数组中任意一个硬盘发生故障时, 仍可读出数据, 在数据重构时, 将数据经计算后重新置入新硬盘中。

以存储网络为中心的存储是全新的存储体系结构。它采用面向网络的存储体系结构, 使数据处理和数据存储分离; 网络存储体系结构包括了网络和 I/O 的精华, 将 I/O 能力扩展到网络上, 特别是灵活的网络寻址能力, 远距离数据传输能力, I/O 高效的原性能; 通过网络连接服务器和存储资源, 消除了不同存储设备和服务器之间的连接障碍; 提高了数据的共享性、可用性、可扩展性和管理性。

1. 网管软件

本知识点主要是让考生了解典型的网络管理平台 and 常用的网络监视器工具。现在网络管理平台有很多，而真正具有 OSI 定义的网管 5 大功能的系统却不多，典型的系统包括 HP 的 Open View、IBM 的 Net View 和 Tivoli、SUN 的 SunNet、Cabletron 的 SPECTRUM。Cisco Work 则是一个最适用于 Cisco 网络设备密集的网络的实用性网络管理系统。

在维护网络时，我们经常需要监视网络数据流并对其进行分析，这也被称为网络监视，而常见的网络监视器包括 Ethereal、NetXRay 和 Sniffer。

(1) Ethereal: 提供了对 TCP、UDP、SMB、Telnet、FTP 等常用协议的支持，覆盖了大部分应用需求。

(2) NetXRay: 主要是用做以太网上的网管软件，能够对 IP、NetBEUI、TCP/UDP 等协议进行详细分析。

(3) Sniffer: 它使网络接口处于混杂模式，以截获网络内容。它是最完善、应用最广泛的一种网络监视器。

Sniffer 软件具有如下功能：捕获网络流量进行详细分析；利用专家分析系统诊断问题，实时监控网络活动；收集网络利用率和错误等。

① 译码分析

如图 10-3 所示是对捕获报文进行解码的显示，通常分为 3 部分。

② 据报文分层

如图 10-4 所示，对于 4 层网络结构，其不同层次完成不同的功能。每一层由众多协议组成。

如图 10-3 所示，在 Sniffer 的解码表中分别对每一层协议进行解码分析。链路层对应“DLC”；网络层对应“IP”；传输层对应“UDP”；应用层对应的是“NETB”等高层协议。

③ 以太网报文结构

Ethernet II 以太网帧类型报文结构为：目的 MAC 地址（6 Bytes）+源 MAC 地址（6 Bytes）+上层协议类型（2 Bytes）+数据字段（46~1500 Bytes）+校验（4 Bytes）。

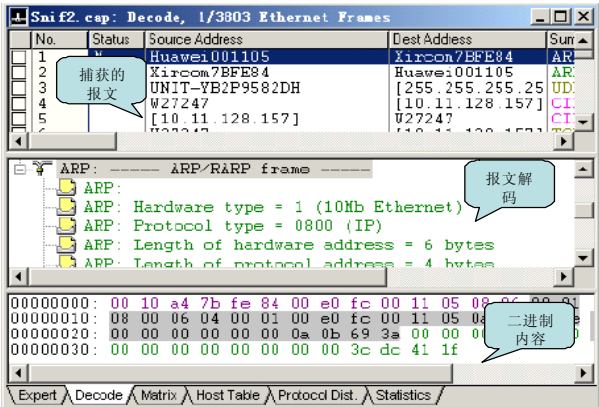


图 10-3 报文捕获与解码

应用层	Telnet、FTP 和 E-mail 等
传输层	TCP 和 UDP
网络层	IP、ICMP、IGMP
链路层	设备驱动程序及接口卡

DLC: Ethernertype=0800, size=229 bytes

IP: D=[10.65.64.255] S=[10.65.64.140] LEN=195 ID=4372

UDP: D=138 S=138 LEN=195

NETB: D=XXYC(1E) S=CWK2 Datagram, 105 bytes (of 173)

CIFS/SMB: C Transaction

SNBNSP: Write mail slot \MAILSLOT-BROWSE

BROWSER: Election Force

图 10-4 数据报文分层

以太网报文结构如图 10-5 所示。

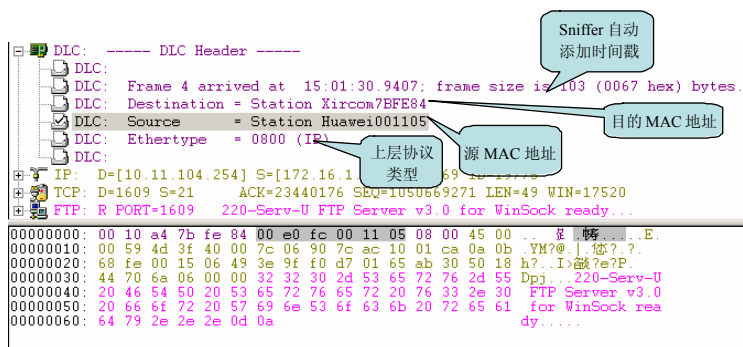


图 10-5 以太网报文结构

源目的 MAC 地址在解码框中可以将前 3 个字节代表厂商的字段翻译出来，方便定位。例如，网络上有两台设备的 IP 地址设置冲突，可以通过解码翻译出厂商信息，方便地找到故障设备，如 00e0fc 为华为，010042 为 Cisco 等。如果需要查看详细的 MAC 地址，用鼠标在解码框中单击此 MAC 地址，在下面的表格中会突出显示该地址的十六进制编码。对于 IP 网络来说，Ether type 字段承载的是上层协议的类型，主要包括：0x800 为 IP 协议，0x806 为 ARP 协议。

④ IEEE 802.3 以太网报文结构

如图 10-6 所示为 IEEE 802.3 SNAP 帧结构，与 Ethernet II 不同的是：目的和源地址后面的字段代表的不是上层协议类型而是报文长度，并多了 LLC 子层。

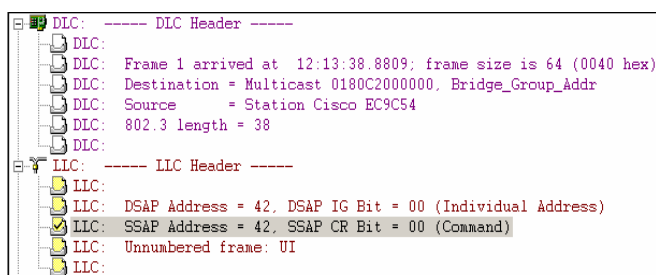


图 10-6 IEEE 802.3 以太网报文

⑤ IP 协议

IP 报文结构为：IP 协议头+载荷。其中对 IP 协议头部的分析，是分析 IP 报文的主要内容之一。下面给出了 IP 协议头部的结构。

IP 协议头部的结构介绍如下。

版本：4——IPv4。

首部长度的单位为 4 字节，最大为 60 字节。

TOS：IP 优先级字段。

总长度：单位是字节，最大 65535 字节。

标识：IP 报文标识字段。

标志：占 3 比特，只用到低位的两个比特。

MF：即 More Fragment，MF=1，代表后面还有分片的数据报；MF=0，代表分片数据报

的最后一个。

DF：即 Don't Fragment，DF=1，代表不允许分片；DF=0，代表允许分片。

段偏移：分片后的分组在原分组中的相对位置，总共 13 比特，单位为 8 字节。

寿命：TTL（Time To Live），丢弃 TTL=0 的报文。

协议：指携带的是何种协议报文（1 代表 ICMP；6 代表 TCP；17 代表 UDP；89 代表 OSPF）。

头部检验和：对 IP 协议首部的校验和。

源 IP 地址：IP 报文的源地址。

目的 IP 地址：IP 报文的地址。

如图 10-7 所示为 Sniffer 对 IP 协议首部的解码分析结构，和 IP 首部各个字段相对应，并给出了各个字段值所表示含义的英文解释。如报文协议（Protocol）字段的编码为 0x11，通过 Sniffer 解码分析转换为十进制数的 17，代表 UDP 协议。其他字段的解码含义与此类似，只要对协议理解得比较清楚，对解码内容的理解也将会变得很容易。

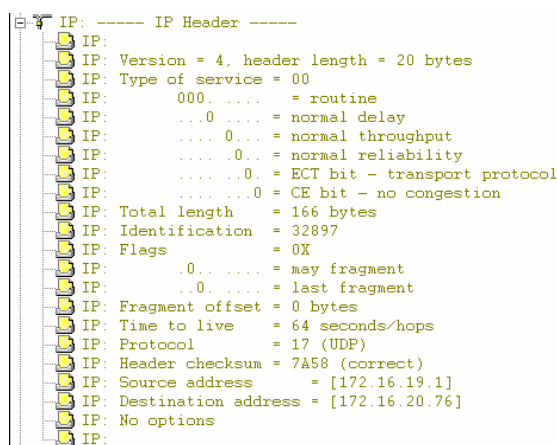


图 10-7 IP 协议首部

2. 数据备份与恢复

本知识点主要是让考生了解数据备份的基本功能以及 3 种典型的策略。在历年考题中还没有出现过直接相关的题目。

数据备份和数据恢复的目的在于最大限度地降低系统风险，保护网络最重要的资源——数据，在系统遇到灾难后，能够提供一种简捷、有效的手段来恢复整个网络。

数据备份和数据恢复的基本功能包括：文件备份和恢复、数据备份和恢复、系统灾难的恢复、备份任务的管理。

常见的数据备份策略包括以下 3 种方式，通常是有机地结合使用，以发挥出最佳的效果。

- (1) 完全备份：备份系统中所有的数据。
- (2) 增量备份：只备份上一次备份后有变化的数据。
- (3) 差分备份（也称为累计备份）：是指备份上一次完全备份以后有变化的数据。

使用时，通常是分三个周期执行：例如每年完全备份一次、每季度差分备份一次、每月增量备份一次。

3. RAID

廉价磁盘冗余阵列 (Redundant Array of Inexpensive Disks, RAID) 技术旨在缩小日益扩大的 CPU 速度和磁盘存储器速度之间的差距。其策略是用多个较小的磁盘驱动器替换单一的大容量磁盘驱动器,同时合理地在多个磁盘上分布存放数据以支持同时从多个磁盘进行读写,从而改善系统的 I/O 性能。最初, inexpensive 一词主要是针对当时另一种技术 (Single Large Expensive Disk, SLED) 而言的,但随着技术的发展, SLED 已是明日黄花, RAID 和 non-RAID 皆采用了类似的磁盘技术。因此 RAID 现在代表独立磁盘冗余阵列 (Redundant Array of Independent Disks), 用 independent 来强调 RAID 技术所带来的性能改善和更高的可靠性。

RAID 机制中共分 8 个级别, RAID 应用的主要技术有分块技术、交叉技术和重聚技术。

(1) RAID 0 级 (无冗余和无校验的数据分块): 具有最高的 I/O 性能和最高的磁盘空间利用率, 其易管理, 但系统的故障率高, 属于非冗余系统, 主要应用于那些关注性能、容量和价格而不是可靠性的应用程序。

(2) RAID 1 级 (磁盘镜像阵列): 由磁盘对组成, 每一个工作盘都有其对应的镜像盘, 上面保存着与工作盘完全相同的数据副本, 具有最高的安全性, 但磁盘空间利用率只有 50%。RAID 1 主要用于存放系统软件、数据以及其他重要文件。它提供了数据的实时备份, 一旦发生故障所有的关键数据即刻就可使用。

(3) RAID 2 级 (采用纠错海明码的磁盘阵列): 采用了海明码纠错技术, 用户需要增加校验盘来提供单纠错和双验错功能。对数据的访问涉及阵列中的每一个盘。大量数据传输时 I/O 性能较高, 但不利于小批量数据传输, 其在实际应用中很少使用。

(4) RAID 3 和 RAID 4 级 (采用奇偶校验码的磁盘阵列): 把奇偶校验码存放在一个独立的校验盘上。如果有一个盘失效, 其上的数据可以通过对其他盘上的数据进行异或运算得到。其读数据很快, 但因为写入数据时要计算校验位, 速度较慢。

(5) RAID 5 (无独立校验盘的奇偶校验码磁盘阵列): 与 RAID 4 类似, 但没有独立的校验盘, 校验信息分布在组内所有盘上, 对于大批量和小批量数据的读写性能都很好。RAID 4 和 RAID 5 使用了独立存取技术, 阵列中每一个磁盘都相互独立地操作, I/O 请求可以并行处理。所以, 该技术非常适合于 I/O 请求率高的应用, 而不太适合于要求高数据传输速率的应用。与其他方案类似, RAID 4、RAID 5 也应用了数据分块技术, 但块的尺寸相对大一些。

(6) RAID 6 (具有独立的数据硬盘与两个独立的分布式校验方案): 在 RAID 6 级的阵列中设置了一个专用的、可快速访问的异步校验盘。该盘具有独立的数据访问通路, 但其性能改进有限, 价格却很昂贵。

(7) RAID 7 (具有最优化的异步高 I/O 速率和高数据传输速率的磁盘阵列): 是对 RAID 6 的改进。在这种阵列中的所有磁盘, 都具有较高的传输速度, 有着优异的性能, 是目前最高档次的磁盘阵列。

(8) RAID 10 (高可靠性与高性能的组合): 由多个 RAID 等级组合而成, 建立在 RAID 0 和 RAID 1 基础上。RAID 1 是一个冗余的备份阵列, 而 RAID 0 是负责数据读写的阵列, 因此又称为 RAID 0+1。由于利用了 RAID 0 极高的读写效率和 RAID 1 较高的数据保护及恢复能力, 使 RAID 10 成为一种性价比较高的等级, 目前几乎所有的 RAID 控制卡都支持这一等级。

4. 网络存储 SAN 与 NAS

网络存储是指建立在客户端-服务器计算的基础上, 将管理和存储文件系统的负担分摊在计算机系统和存储设备之间。由计算机负责数据的处理, 存储设备或子系统负责数据的存

储。网络存储利用专用的存储服务器和存储子系统实现,负责在多个系统间分配存储任务,在一个或多个位置实现简单而可靠的数据存储,从一个或多个位置实现简单而可靠的数据恢复。

存储连接技术最新的发展包括网络连接存储(NAS)、存储区域网络(SAN)和光纤路径三种,其中NAS和SAN在概念上相对复杂。

(1) NAS: 将存储设备连接到现有网络上,提供数据和文件服务。一般由存储硬件、操作系统以及其上的文件系统等几个部分组成。它通常不依赖于通用操作系统,而是采用面向用户设计、专用于数据存储的简化操作系统。NAS与客户间通信通常使用NFS协议、CIFS协议。

(2) SAN: 存储区域网络是一种专用网络,可以把一个或多个系统连接到存储设备和子系统。与NAS相比,SAN具有无限的扩展能力、更高的连接速度和处理能力。

10.4.2 一点一练

试题 1

使用RAID作为网络存储设备有许多好处,下列关于RAID的叙述中不正确的是__(1)___。

- (1) A. RAID使用多块廉价磁盘阵列构成
- B. RAID采用交叉存取技术,提高了访问速度
- C. RAID 0使用磁盘镜像技术,提高了可靠性
- D. RAID 3利用一个奇偶校验盘完成容错功能,减少了冗余磁盘数量

试题 2

嗅探器可以使网络接口处于杂收模式,在这种模式下,网络接口__(2)___。

- (2) A. 只能响应与本地网络接口硬件地址相匹配的数据帧
- B. 只能响应本网段的广播数据帧
- C. 只能响应组播信息
- D. 能够响应流经网络接口的所有数据帧

试题 3

计算机系统中广泛采用了RAID技术,在各种RAID技术中,磁盘容量利用率最低的是__(3)___。

- (3) A. RAID 0 B. RAID 1 C. RAID 3 D. RAID 5

试题 4

下面关于几个网络管理工具的描述中,错误的是__(4)___。

- (4) A. netstat 可用于显示IP、TCP、UDP、ICMP等协议的统计数据
- B. sniffer 能够使网络接口处于杂收模式,从而可截获网络上传输的分组
- C. winipcfg 用MS-DOS工作方式显示网络适配器和主机的有关信息
- D. tracert 可以发现数据报到达目标主机所经过的路由器和到达时间

试题 5

嗅探器改变了网络接口的工作模式,使得网络接口__(5)___。

- (5) A. 只能响应发送给本地的分组
- B. 只能响应本网段的广播分组
- C. 能够响应流经网络接口的所有分组
- D. 能够响应所有组播信息

10.4.3 解析与答案

试题 1 分析

本题考查 nslookup 命令。

廉价磁盘冗余阵列 (Redundant Array of Inexpensive Disks, RAID) 是由美国加利福尼亚大学伯克利分校在 1987 年提出的, 现在已经广泛应用在大、中型计算机和计算机网络储存系统中。它是利用一台磁盘阵列控制器来管理和控制一组磁盘驱动器, 组成一个高度可靠、快速的大容量磁盘系统。

RAID 根据访问速度和可靠性分成很多级别。

① RAID 0: 没有容错设计的条带磁盘阵列 (Striped Disk Array without Fault Tolerance), 仅提供并行交叉存取功能。它虽能有效地提高磁盘 I/O 速度, 但是磁盘系统的可靠性不好。

② RAID 1: 具有磁盘镜像和双工 (Mirroring and Duplexing) 功能, 可利用并行读/写特性, 将数据块同时写入主盘和镜像盘, 比传统的镜像盘速度快, 但磁盘利用率只有 50%。

③ RAID 2: 增加了汉明码校验与纠错 (Hamming Code ECC) 功能, 是早期为了进行即时数据校验而研制的一种技术, 针对当时对数据安全敏感领域, 如金融服务等。但由于花费太大, 造成成本昂贵, 目前已不再使用。

④ RAID 3: 具有并行传输和校验 (Parallel Transfer with Parity) 功能的磁盘阵列。它利用一台奇偶校验盘来完成容错功能。比起磁盘镜像, 减少了所需的冗余磁盘数。

⑤ RAID 4: 具有独立的数据硬盘与共享的校验硬盘 (Independent Data Disks with Shared Parity Disk), 与 RAID 3 相比, RAID 4 是一种相对独立的形式。

⑥ RAID 5: 具有独立的数据磁盘和分布式校验块 (Independent Data Disks with Distributed Parity Blocks) 的磁盘阵列。每个驱动器都有独立的数据通路, 独立地进行读/写, 无专门的校验盘, 用于纠错的校验信息是以螺旋方式散布在所有数据盘上。RAID 5 常用于 I/O 较频繁的事务处理上。

⑦ RAID 6: 具有独立的数据硬盘与两个独立的分布式校验方案 (Independent Data Disks with Two Independent Distributed Parity Schemes)。在 RAID 6 级的阵列中设置了一个专用的、可快速访问的异步校验盘。该盘具有独立的数据访问通路, 但其性能改进有限, 价格却很昂贵。

⑧ RAID 7: 具有最优化的异步高 I/O 速率和高数据传输率 (Optimized Asynchrony for High I/O Rates as well as High Data Transfer Rates) 的磁盘阵列, 是对 RAID 6 级的改进。在这种阵列中的磁盘都具有较高的传输速度, 以及优异的性能, 是目前最高档次的磁盘阵列。

⑨ RAID 10: 高可靠性与高性能的组合 (Very High Reliability combined with High Performance)。这种 RAID 是由多个 RAID 等级组合而成, 而不像 RAID 5 那样是全新的等级。RAID 10 是建立在 RAID 0 和 RAID 1 基础上的, RAID 1 是一个冗余的备份阵列, 而 RAID 0 是负责数据读写的阵列, 因此被很多人称为 RAID 0+1。由于利用 RAID 0 级较高的读写效率和 RAID 1 级较高的数据保护和恢复能力, 使 RAID 10 成为一种性价比较高的等级, 目前几乎所有的 RAID 控制卡都支持这一等级。

试题 1 答案

(1) C

试题 2 分析

在一般情况下, 网络上所有的计算机都可以接收到通过的数据帧, 但对不属于自己的报文则不予响应, 但是如果某工作站的网络接口处于杂收模式, 那么它就可以捕获网络上所有的报文和帧, 如果一工作站被配置成这样的方式, 它就是一个嗅探器。

试题 2 答案

(2) D

试题 3 分析

RAID 是 Redundant Arrays of Independent Disks 的简称, 中文为廉价冗余磁盘阵列。

① RAID 0: 将多个较小的磁盘合并成一个大的磁盘, 不具有冗余, 速度最快, 但可靠性最差。

② RAID 1: 两组相同的磁盘系统互作镜像, 速度没有提高, 但是允许单个磁盘出错, 可靠性最好, 但是其磁盘的利用率却只有 50%, 是所有 RAID 上磁盘利用率最低的一个级别。

③ RAID 3: 其存放数据的原理和 RAID 0、RAID 1 不同。RAID 3 是以一个硬盘来存放数据的奇偶校验位, 数据分段存储于其余硬盘中。利用单独的校验盘来保护数据虽然没有镜像的安全性高, 但是硬盘利用率得到了很大的提高, 为 $n-1$ 。

④ RAID 5: 向阵列中的磁盘写数据, 奇偶校验数据存放在阵列中的各个盘上, 允许单个磁盘出错。RAID 5 也是以数据的校验位来保证数据的安全, 但它不是以单独硬盘来存放数据的校验位, 而是将数据段的校验位交互存放于各个硬盘上。这样, 任何一个硬盘损坏, 都可以根据其他硬盘上的校验位来重建损坏的数据。硬盘的利用率为 $n-1$ 。

试题 3 答案

(3) B

试题 4 分析

netstat (network statistics) 是一个命令行工具, 用于显示网络连接、路由表和网络端口收发数据报的统计信息等。

* netstat -a: 显示所有连接和监听端口。

* netstat -e: 显示以太网统计信息。

* netstat -n: 以数字形式显示网络地址和端口号。

* netstat -r: 显示路由表。

* netstat -s: 按协议显示统计信息, 包括 IP、ICMP、TCP 和 UDP 等。

tracert 命令的作用是跟踪数据报到达目标主机的路径, 如果发现网络不通, 可以用 tracers 跟踪数据报传输的路径, 发现出故障的节点。例如:

```
tracert www.263.net
```

```
Tracing route to www.263.net [211.100.31.131] (解析出 www.263.net 的主机 IP 地址)
```

```
over a maximum of 30 hops:
```

```
1 1 ms 2 ms 2 ms 202.201.3.1
```

```
2 2 ms 2 ms 2 ms 210.202.88.126
```

```
3 3 ms 4 ms 4 ms 210.112.46.13
```

```
4 5 ms 5 ms 6 ms 210.112.46.149
```

```
5...Request timed out. (从 202.112.46.149 到上一级路由器之间发生了故障)
```

winipcfg 与 ipconfig 功能一样, 用于显示主机中 IP 协议的配置信息, winipcfg 适用于 Windows 95/98, 而 ipconfig 适用于 Windows NT/2000/XP。winipcfg 不使用参数, 它以 Windows 窗口形式显示网络适配器的物理地址、主机 IP 地址、子网掩码及默认网关等配置信息。单击其中的“其他信息”按钮, 可以查看主机名、DNS 服务器和节点类型等。

sniffer 是一类程序的总称, 即嗅探器, 它可以通过计算机的网络接口, 接收网络中传输的各种数据报, 从而进行协议分析和通信流分析, 解决网络维护和管理方面的问题。安装了 sniffer 的计算机, 其网卡被设置为杂收 (promiscuous) 模式, 这样就能截获网络上传的任何数据报。与通常情况下的网卡不一样, 通常的网卡默认只接收发送给自己的数据报, 嗅探

器可能被合法地使用,也可能被恶意地使用,网络黑客利用嗅探器程序,可以根据截获的数据报发现用户的账户信息,从而实施网络攻击活动。Sniffer(首写字母大写)是 Network Genera 公司开发的最早的分组捕获和代码分析软件,用于网络通信分析和故障排除。

试题 4 答案

(4) C

试题 5 分析

嗅探器是一种监视网络数据运行的软件设备,其改变了网络接口的工作模式,使得网络接口能够响应流经网络接口的所有分组。

试题 5 答案

(5) C

10.5 考前冲刺

试题 1

SNMPv1 的管理信息结构定义的应用数据类型 time ticks 的单位是____(1)____。

(1) A. 1 秒 B. 0.1 秒 C. 0.01 秒 D. 1 毫秒

试题 2

某校园网用户无法访问外部站点 210.102.58.74,管理人员在 Windows 操作系统下可以使用____(2)____判断故障发生在校园网内还是校园网外。

(2) A. ping 210.102.58.74 B. tracert 210.102.58.74
C. netstat 210.102.58.74 D. arp 210.102.58.74

试题 3

在 Windows 操作系统中,如果要查找从本地出发,经过 3 个跳步,到达名字为 Enric 的目标主机的路径,则输入的命令是____(3)____。

(3) A. tracert Enric-h 3 B. tracert -j 3 Enric
C. tracert -h 3 Enric D. tracert Enric -j 3

试题 4

能显示 TCP 和 UDP 连接信息的命令是____(4)____。

(4) A. netstat -s B. netstat -e C. netstat -r D. netstat -a

试题 5

在 Windows 操作系统中,采用____(5)____命令来测试到达目标所经过的路由器数目及 IP 地址。

(5) A. ping B. tracert C. arp D. nslookup

试题 6

在 Linux 操作系统中,____(6)____文件负责配置 DNS,它包含了主机的域名搜索顺序和 DNS 服务器的地址。

(6) A. /etc/hostname B. /etc/host.conf
C. /etc/resolv.conf D. /etc/name.conf

试题 7

Linux 系统在默认情况下将创建的普通文件的权限设置为____(7)____。

(7) A. -rw-r-r- B. -r-r-r- C. -rw-rw-rwx D. -rwxrwxrwx

试题 8

在 Linux 系统中, 用户组加密后的口令存储在____(8)____文件中。

- (8) A. /etc/passwd B. /etc/shadow C. /etc/group D. /etc/shells

试题 9

以下关于 Windows Server 2003 的域管理模式的描述中, 正确的是____(9)____。

- (9) A. 域间信任关系只能是单向信任
B. 单域模型中只有一个主域控制器, 其他都为备份域控制器
C. 每个域控制器都可以改变目录信息, 并把变化的信息复制到其他域控制器
D. 只有一个域控制器可以改变目录信息

试题 10

在 Windows Server 2003 中, 默认情况下____(10)____组用户拥有访问和完全控制终端服务器的权限。

- (10) A. Interactive B. Network C. Everyone D. System

试题 11

在 Linux 系统中, 利用____(11)____命令可以分页显示文件的内容。

- (11) A. list B. cat C. more D. cp

试题 12

SNMP 采用 UDP 提供数据报服务, 这是由于____(12)____。

- (12) A. UDP 比 TCP 更加可靠
B. UDP 数据报文可以比 TCP 数据报文大
C. UDP 是面向连接的传输方式
D. 采用 UDP 实现网络管理不会太多增加网络负载

试题 13

在 SNMPv2 中, 一个实体发送一个报文, 一般经过 4 个步骤:

- ① 加入版本号和团体名, 构造报文;
② 把 PDU、源和目标端口地址以及团体名传送给认证服务, 认证服务产生认证码或对数据进行加密, 返回结果;
③ 根据要实现的协议操作构造 PDU;
④ 进行 BER 编码, 产生 0/1 比特串。
这 4 个步骤的正确次序是____(13)____。

- (13) A. ①③②④ B. ③②①④ C. ④①③② D. ②①③④

试题 14

活动目录 (Active Directory) 是由组织单元、域、____(14)____和域森林构成的层次结构, 安装活动目录要求分区的文件系统为____(15)____。

- (14) A. 超域 B. 域树 C. 团体 D. 域控制器
(15) A. FAT16 B. FAT32 C. ext2 D. NTFS

试题 15

在网络管理中要防范各种安全威胁。在 SNMPv3 中, 不必要或无法防范的安全威胁是____(16)____。

- (16) A. 篡改管理信息: 通过改变传输中的 SNMP 报文实施未经授权的管理操作
B. 通信分析: 第三者分析管理实体之间的通信规律, 从而获取管理信息

- C. 假冒合法用户：未经授权的用户冒充授权用户，企图实施管理操作
- D. 消息泄露：SNMP 引擎之间交换的信息被第三者偷听

试题 16

在 Windows XP 中用事件查看器查看日志文件，可看到的日志包括____(17)_____。

- (17) A. 用户访问日志、安全性日志和系统日志
- B. 应用程序日志、安全性日志和系统日志
- C. 网络攻击日志、安全性日志和记账日志
- D. 网络连接日志、安全性日志和服务日志

试题 17

在 Linux 中，可以利用____(18)_____命令来终止某个进程。

- (18) A. kill B. dead C. quit D. exit

试题 18

下面有关 RMON 的论述中，错误的是____(19)_____。

- (19) A. RMON 的管理信息库提供整个子网的管理信息
- B. RMON 的管理信息库属于 MIB-2 的一部分
- C. RMON 监视器可以对每个分组进行统计和分析
- D. RMON 监视器不包含 MIB-2 的功能

试题 19

SNMPv2 提供了 3 种访问管理信息的方法，这 3 种方法不包括____(20)_____。

- (20) A. 管理站向代理发出通信请求 B. 代理向管理站发出通信请求
- C. 管理站与管理站之间的通信 D. 代理向管理站发送陷入报文

试题 20

SNMPv1 使用____(21)_____进行报文认证，这个协议是不安全的。SNMPV2 定义了____(22)_____的安全模型，可以使用共享密钥进行报文认证。

- (21) A. 版本号 (Version) B. 协议标识 (Protocol ID)
- C. 团体名 (Community) D. 制造商标识 (Manufacturer ID)
- (22) A. 基于用户 B. 基于共享密钥
- C. 基于团体 D. 基于报文认证

试题 21

网络管理的 5 大功能域是____(23)_____。

- (23) A. 配置管理、故障管理、计费管理、性能管理和安全管理
- B. 配置管理、故障管理、计费管理、带宽管理和安全管理
- C. 配置管理、故障管理、成本管理、性能管理和安全管理
- D. 配置管理、用户管理、计费管理、性能管理和安全管理

试题 22

在 Windows 系统中，默认权限最低的用户组是____(24)_____。

- (24) A. Everyone B. Administrators C. Power Users D. Users

试题 23

与 route print 具有相同功能的命令是____(25)_____。

- (25) A. ping B. arp-a C. netstat-r D. tracert-d

试题 24

在下面的 Linux 系统中，能关闭系统的命令是____(26)____。

- (26) A. kill B. shutdown C. exit D. logout

试题 25

在 Linux 系统中，更改用户口令的命令是____(27)____。

- (27) A. pwd B. passwd C. kouling D. password

试题 26

在 Linux 系统中，目录“/proc”主要用于存放____(28)____。

- (28) A. 设备文件 B. 命令文件
C. 配置文件 D. 进程和系统信息

试题 27

在 Linux 系统中，某文件的访问权限信息为“-rwxr--r--”，以下对该文件的说明中，正确的是____(29)____。

- (29) A. 文件所有者有读、写和执行权限，其他用户没有读、写和执行权限
B. 文件所有者有读、写和执行权限，其他用户只有读权限
C. 文件所有者和其他用户都有读、写和执行权限
D. 文件所有者和其他用户都只有读和写权限

试题 28

下面关于域本地组的说法中，正确的是____(30)____。

- (30) A. 成员可来自森林中的任何域，仅可访问本地域内的资源
B. 成员可来自森林中的任何域，可访问任何域中的资源
C. 成员仅可来自本地域，仅可访问本地域内的资源
D. 成员仅可来自本地域，可访问任何域中的资源

试题 29

在 SNMPv3 中，把管理站 (Manager) 和代理 (Agent) 统一叫____(31)____。

- (31) A. SNMP 实体 B. SNMP 引擎 C. 命令响应器 D. 命令生成器

试题 30

默认情况下，Linux 系统中用户登录密码信息存放在____(32)____文件中。

- (32) A. /etc/group B. /etc/userinfo C. /etc/shadow D. /etc/profile

10.6 习题解析

试题 1 分析

SMI 定义了 SNMP 框架所用信息的组织、组成和标识，它还为描述 MIB 对象和描述协议怎样交换信息奠定了基础。SMI 的数据类型主要有 3 种：简单类型 (simple)、简单结构类型 (simple-constructed) 和应用类型 (application-wide)。其中应用数据类型采用隐式定义，是引用 SNMP 的简单数据类型来定义的，主要有 6 种：① IP-Address，以网络序表示的 IP 地址，因为它是一个 32 位的值，所以定义为 4 个字节；② network address，网络地址，表示从一个特定协议族中选定的网络地址，SNMPv1 仅支持 32 位的 IP 地址，所以与 IPAddress 等效；③ counter，计数器是一个非负的整数，它递增至最大值，而后归零。SNMPv1 中定义的计数器是 32 位的，即最大值为 4, 294, 967, 295；④ Gauge，也是一个非负整数，它可以递增或递减，但达到最大值时保持在最大值，其最大值为 $2^{32}-1$ ；⑤ time ticks，是一个

时间单位，表示以 0.01 秒为单位计算的时间；⑥ opaque，表示用于传递任意信息串的任何编码格式，它与 SMI 使用的严格数据输入格式不同。

试题 1 答案

(1) C

试题 2 分析

当网络无法访问外部站点时，采用 ping 操作只能判断用户与外部站点的连通性，但是无法判断故障处于校园网内还是校园网外；而 netstat 用于显示与 IP、TCP、UIIP 和 ICMP 协议相关的统计数据，一般用于检验本机各端口的网络连接情况，且 C 选项中的命令格式不对；使用 arp 可以查看和修改本地计算机上的 arp 表项。arp 命令对于查看 arp 缓存和解决地址解析问题非常有用；而使用 tracert 可以跟踪网络连接，tracert（跟踪路由）是路由跟踪实用程序，用于确定 IP 数据报访问目标所采取的路径。通过该命令可以查看在哪段路由出现连通问题。

试题 2 答案

(2) B

试题 3 分析

tracert 命令的用法如下：

```
tracert [-d] [-h maximum_hops] [-j hop-list] [-w timeout] <target name>
```

其中：

- d 不将 IP 地址解析成主机名；
- h max-hops 指定了最大跟踪跳步数；
- j hop-list 指定了有限源路由；
- w timeout 指定了响应的超时时间，单位是毫秒。

试题 3 答案

(3) C

试题 4 分析

netstat 命令的用法如下：

```
netstat [-a] [-e] [-n] [-s] [-p proto] [-r] [interval]
```

其中：

- a 显示所有连接和处于监听状态的接口（服务器端的连接通常不显示）；
- c 显示所有以太网统计数据。这个选项可以与-s 选项一起使用；
- n 用数字的形式显示地址和端口号；
- p proto 显示 proto 指定协议的连接，proto 的取值可以是 TCP 或 UDP，如果配合-s 选项则可以显示每个协议的统计数据，proto 的取值可以是 TCP、UDP 或 IP；
- r 显示路由表的内容；
- s 显示每个协议的统计数据，默认显示 TCP、UDP 和 IP 的统计数据，利用-p 选项可以指定只显示其中一部分；

interval 每隔 interval 秒重复显示指定的统计数据，按 Ctrl+C 组合键可终止显示，如果不指定 interval，netstat 会将当前的信息显示一次。

试题 4 答案

(4) D

试题 5 分析

ping 是 Windows 系列自带的一个可执行命令，用于验证与远程计算机的连接。该命令只有在安装了 TCP/IP 协议后才可以使⽤。ping 命令的主要作用是通⽬过发送数据报并接收应⽬答信息来检测两台计算机之间的网络是否连通。当网络出现故障时，可以⽬用这个命令来预测故障和确定故障地点。ping 命令成功只是说明当前主机与⽬目的主机之间存在一条连通的路径。如果不成功，则考虑网线是否连通、网卡设置是否正确、IP 地址是否可用等。利⽬用它可以检查网络是否能够连通。ping 命令应⽬用格式为 ping IP 地址。该命令还可以添加参数使⽬用，输入 ping 按 Enter 键即可看到详细说明。

tracert 命令主要用来显示数据包到达⽬目的主机所经过的路径。该命令的使⽬用格式是在 DOS 命令提示符下或者直接在“运行”对话框中输入如下命令：tracert 主机 IP 地址或主机名。执行结果返回数据报到达⽬目的主机前所经历的中继站清单，并显示到达每个中继站的时间。该功能同 ping 命令类似，但它所看到的信息要比 ping 命令详细得多，它把⽬用户送出的到某一站点的请求包，所走的全部路由都告诉⽬用户，并且告诉⽬用户通过该路由的 IP 是多少，通过该 IP 的时延是多少。具体的 tracert 命令后还可跟参数，输入 tracert 后按 Enter 键，会显示很详细的说明。

arp 命令用以显示和修改“地址解析协议（ARP）”缓存中的项目。ARP 缓存中包含一个或多个表，它们用于存储 IP 地址及其经过解析的以太网或令牌环物理地址。计算机上安装的每一个以太网或令牌环网络适配器都有自己单独的表。如果在没有参数的情况下使用，则 arp 命令将显示帮助信息。语法如下：

```
arp[-a [InetAddr] [-N IfaceAddr]] [-g[InetAddr] [-N IfaceAddr]] [-d InetAddr[IfaceAddr]] [-s InetAddr EtherAddr [IfaceAddr]]
```

nslookup 命令的功能是查询一台机器的 IP 地址和其对应的域名。它通常需要一台域名服务器来提供域名服务。如果用户已经设置好域名服务器，就可以用这个命令查看不同主机的 IP 地址对应的域名。

该命令的一般格式为：nslookup [IP 地址/域名]。

试题 5 答案

(5) B

试题 6 分析

在 Linux 操作系统中，/etc/hostname 文件包含了 Linux 系统的主机名称，包括完全的域名；/etc/host.conf 文件指定如何解析主机域名，Linux 通过解析库来获得主机名对应的 IP 地址；/etc/resolv.conf 文件负责配置 DNS，它包含了主机的域名搜索顺序和 DNS 服务器的地址。

试题 6 答案

(6) C

试题 7 分析

Linux 系统对文件的访问设定了三级权限：文件所有者，文件所有者同组的用户和其他用户；同时对文件的访问做三种处理操作：读取、写入和执行。Linux 文件被创建时，文件所有者可以对该文件的权限进行设置。在默认情况下，系统将创建的普通文件的权限设置为 -rw-r-r-

试题 7 答案

(7) A

试题 8 分析

/etc/passwd 文件是 Linux 系统中用于用户管理的重要文件，这个文件对所有用户都是可读的，Linux 系统中的每个用户在/etc/passwd 文件中都有一行对应的记录，用户在登录时，会先在/etc/passwd 文件中找到用户 ID。/etc/passwd 保存着加密后的用户口令。而/etc/group 是管理用户组的基本文件，在/etc/group 中每行记录对应一个组，它包括用户组名，加密后的组口令，组 ID 和组成员列表。

试题 8 答案

(8) C

试题 9 分析

Windows Server 2003 采用了活动目录技术，域间信任关系有多种形式，在 Windows Server 2003 中采用了多主机复制模式，多个域控制器没有主次之分。域中每个域控制器即可接收其他域控制器的变化信息而改变目录信息，也可把变化的信息复制到其他域控制器。

试题 9 答案

(9) C

试题 10 分析

Windows Server 2003 在系统安装完毕后，会自动建立几个特殊组，其中包括 Interactive（任何在本机登录的用户）、Network（任何通过网络连接的用户）、Everyone（任何使用计算机的人员）和 System（系统组）等。而终端服务可以让操作者通过远程访问服务器桌面。在默认情况下，只有系统管理员组（Administrators）和系统组用户（System）拥有访问和完全控制终端服务器的权限。

试题 10 答案

(10) D

试题 11 分析

在 Linux 系统中，cat 命令用来在屏幕上滚动显示文件内容；more 命令可以分页显示文件内容；cp 为文件复制命令。

试题 11 答案

(11) C

试题 12 分析

SNMP 定义为依赖于 UDP 数据报服务的应用层协议。SNMP 实体向管理应用程序提供服务，它的作用是把管理应用程序的服务调用变成对应的 SNMP 协议数据单元，并利用 UDP 数据报发送出去。之所以选择 UDP 协议而不是 TCP 协议，是因为 UDP 效率较高，这样实现网络管理时不会太多地增加网络负载。但由于 UDP 不可靠，所以 SNMP 报文容易丢失。为此，对 SNMP 实现的是将每个管理信息装配成单独的数据报独立发送，而且报文较短，不超过 484 个字节。

试题 12 答案

(12) D

试题 13 分析

在 SNMPv2 中，一个实体发送一个报文一般要经过下面 4 个步骤。

- ① 根据要实现的协议操作构造 PDU；
- ② 把 PDU、源和目标端口地址以及团体名传送给认证服务，认证服务产生认证码或对

数据进行加密, 返回结果;

- ③ 加入版本号和团体名, 构造报文;
- ④ 进行 BER 编码, 产生 0/1 比特串, 发送出去。

试题 13 答案

(13) B

试题 14 分析

活动目录以对象的形式存储网络元素的信息, 如计算机、用户等。一个对象就是一个类的实例。面向对象的存储机制保证了对象数据的安全性。Windows 的活动目录逻辑单元包括组织单元 (OU)、域 (Domain)、域树 (Tree) 和域森林 (Forest), 它们构成 T 层次的结构。域森林由域树组成, 域树又由域组成, 域中的对象可以按 OU 划分。OU 负责把对象组织起来。

域为活动目录的核心单元, 为容器对象, 它是一些基本对象 (如计算机、用户等) 的容器, 而这些对象有相同的安全需求、复制过程和管理。活动目录中采用 DNS 域名对域进行标记, 如 reskit.com。活动目录为每个域建立一个目录数据库的副本, 这个副本只存储用于这个域的对象。在域控制器之间, 活动目录以多主域复制模型实现目录复制。

组织单元为一个逻辑概念。由于管理上的需要, 把域内的对象组织成逻辑组, 如用户组、打印机组等。OU 也是一个对象的容器, 用来组织、管理一个域内的对象, 但 OU 不能包括来自其他域的对象。OU 可以包含各种对象, 比如用户账户、用户组、计算机、打印机等, 甚至可以包括其他的 OU, 所以可以利用 OU 把域中的对象形成一个完全逻辑上的层次结构。

由域所组成的集合, 构成域树。在域树中, 每个域都拥有自己的目录数据库副本来存储自己的对象。如果从根域开始, 每加入一个域, 则新的域就成为树中的一个子域。域树的第一个域是该域树的根 (Root), 域树中的每一个域共享共同的配置、模式对象和全局目录 (Global Catalog)。具有公用根域的所有域构成连续名称空间, 域树上的域共享相同的 DNS 域名后缀, 这就意味着子域的域名就是添加到父域域名中的那个子域的名称。

由域树所组成的集合, 用信任关系相关联, 共享一个公共的目录模式、配置数据和全局目录。域森林中的每一个域树具有自己唯一独立的命名空间。在域森林中创建的第一棵树默认地被创建为该域森林的根树 (Root Tree)。域树和域森林的结构, 可以帮助活动目录使用容器层次结构来模拟一个企业的组织结构。

安装活动目录要求分区的文件系统为 NTFS。

试题 14 答案

(14) B

(15) D

试题 15 分析

SNMPv3 把对网络协议的安全威胁分为主要威胁和次要威胁两类。标准规定安全模块必须提供防范的 4 种主要威胁如下。

① 修改信息 (Modification of Information): 就是某些未经授权的实体改变了 SNMP 报文, 企图实施未经授权的管理操作, 或者提供虚假的管理对象。

② 假冒 (Masquerade): 即未经授权的用户冒充授权用户的标识, 企图实施管理操作。标准还规定安全模块必须对两种次要威胁提供防护。

③ 修改报文流 (Message Stream Modification): 由于 SNMP 协议通常是用于无连接的传输服务, 重新排序报文流、延迟或重放报文的威胁都可能出现。这种威胁的危害性在于通过报文流的修改可能实施非法的管理操作。

④ 消息泄露 (Disclosure): SNMP 引擎之间交换的信息可能被偷听, 对这种威胁的防

范应采取局部的策略。

有两种威胁是安全体系结构不必防范的，因为它们不是很重要，或者这种防范没有多大作用。

① 拒绝服务 (Denial of Service): 因为在很多情况下拒绝服务和网络失效是无法区别的，所以可以由网络管理协议来处理，安全子系统不必采取措施。

② 通信分析 (Traffic Analysis): 即由第三者分析管理实体之间的通信规律。从而获取需要的信息。由于通常都是由少数管理站来管理整个网络的，所以管理系统的通信模式是可预见的，防护通信分析就没有多大作用了。

试题 15 答案

(16) B

试题 16 分析

在桌面上右击“我的电脑”图标，在弹出的快捷菜单中选择“管理”命令，调出计算机管理窗口。事件查看器允许用户监视“应用程序”、“安全性”和“系统”日志中记录的事件。

试题 16 答案

(17) B

试题 17 分析

Linux 下终止进程最安全的方法是单纯使用 kill 命令。首先使用 ps -ef 命令确定要杀死进程的 PID，然后输入命令：# kill -pid，即可终止某个进程。

试题 17 答案

(18) A

试题 18 分析

RMON 监视系统由两部分构成：探测器（代理或监视器）和管理站。RMON 代理在 RMON MIB 中存储网络信息，它们被直接植入网络设备（如路由器、交换机等），代理也可以是 PC 上运行的一个程序。代理只能看到流经它们的流量，所以在每个被监控的 LAN 段或 WAN 链接点都要设置 RMON 代理，网管工作站用 SNMP 获取 RMON 数据信息。

试题 18 答案

(19) D

试题 19 分析

SNMPv2 提供了如下 3 种访问管理信息的方法。

管理站和代理之间的请求/响应通信，这种方法与 SNMPv1 是一样的。

管理站和管理站之间的请求/响应通信，这种方法是 SNMPv2 特有的，可以由一个管理站把有关管理信息告诉另外一个管理站。

代理系统到管理站的非确认通信，即由代理向管理站发送陷入报文，报告出现的异常情况。SNMPv2 中也有对应的通信方式。

试题 19 答案

(20) B

试题 20 分析

SNMPv1 使用团体名进行报文认证，这个协议是不安全的。SNMPv3 定义了基于用户的安全模型 (USM)，可以使用共享密钥进行报文认证。

试题 20 答案

(21) C

(22) A

试题 21 分析

OSI 网络管理标准中的 5 大功能介绍如下。

① 配置管理：自动发现网络拓扑结构，构造和维护网络系统的配置，监测网络被管对象的状态，完成网络关键设备配置的语法检查，配置自动生成和自动配置备份系统，对于配置的一致性进行严格的检验。

② 故障管理：过滤、归并网络事件，有效地发现、定位网络故障，给出排错建议与排错工具，形成整套的故障发现、告警与处理机制。

③ 性能管理：采集、分析网络对象的性能数据，监测网络对象的性能，对网络线路质量进行分析。同时，统计网络运行状态信息，对网络的使用发展做出评测、估计，为网络进一步规划与调整提供依据。

④ 安全管理：结合使用用户认证、访问控制、数据传输、存储的保密与完整性机制，以保障网络管理系统本身的安全。维护系统日志，使系统的使用和网络对象的修改有据可查。控制对网络资源的访问。

⑤ 计费管理：对网际互联设备按 IP 地址的双向流量统计，产生多种信息统计报告及流量对比，并提供网络计费工具，以便用户根据自定义的要求实施网络计费。

试题 21 答案

(23) A

试题 22 分析

Windows 是一个支持多用户、多任务的操作系统，不同的用户在访问这台计算机时，将会有不同的权限。同时，对用户权限的设置也是基于用户和进程而言的，在 Windows 系统里，用户被分成许多组，组和组之间都有不同的权限，并且一个组的用户和用户之间也可以有不同的权限。以下是常见的用户组。

① Users：普通用户组，这个组的用户无法进行有意或无意的改动。因此，用户可以运行经过验证的应用程序，但不可以运行大多数旧版应用程序。Users 组是最安全的组，因为分配给该组的默认权限不允许成员修改操作系统的设置或用户资料。Users 组提供了一个最安全的程序运行环境。在经过 NTFS 格式化的卷上，默认安全设置旨在禁止该组的成员危及操作系统和已安装程序的完整性。用户不能修改系统注册表设置、操作系统文件或程序文件。Users 可以创建本地组，但只能修改自己创建的本地组。Users 可以关闭工作站，但不能关闭服务器。

② Power Users：高级用户组，Power Users 可以执行除了为 Administrators 组保留的任务外的其他任何操作系统任务。分配给 Power Users 组的默认权限允许 Power Users 组的成员修改整个计算机的设置。但 Power Users 不具有将自己添加到 Administrators 组的权限。在权限设置中，这个组的权限是仅次于 Administrators 的。

③ Administrators：管理员组，在默认情况下，Administrators 中的用户对计算机/域有不受限制的完全访问权。分配给该组的默认权限允许对整个系统进行完全控制。一般来说，应该把系统管理员或者与其有着同样权限的用户设置为该组的成员。

④ Guests：来宾组，来宾组与普通组 Users 的成员有同等访问权，但来宾账户的限制更多。

⑤ Everyone：所有的用户，这个计算机上的所有用户都属于这个组。

⑥ System 组：这个组拥有和 Administrators 一样甚至更高的权限，在查看用户组时它不会被显示出来，也不允许任何用户的加入。这个组主要是保证了系统服务的正常运行，赋

予系统及系统服务的权限。

试题 22 答案

(24) A

试题 23 分析

route print 用来查看本机的路由表，和 netstat-r 具有相同的功能。

试题 23 答案

(25) C

试题 24 分析

Linux 下关闭系统的命令有 shutdown 和 init 0 等命令，kill 命令用于终止某个进程，exit 命令可以退出某个 shell，logout 命令可以实现当前用户从系统中注销。

试题 24 答案

(26) B

试题 25 分析

通常在 Linux 系统中，passwd 指令让用户可以更改自己的密码，而系统管理者则能用它管理系统用户的密码。只有管理者可以指定用户名称，一般用户只能变更自己的密码。

试题 25 答案

(27) B

试题 26 分析

/proc 目录，保存了当前系统所有的详细信息，包括进程、文件系统、硬件等。而且还可以通过/proc 来即时修改系统中的某些参数。

试题 26 答案

(28) D

试题 27 分析

在 Linux 系统中，每一个文件和目录都有相应的访问许可权限，文件或目录的访问权限分为可读（可列目录）、可写（对目录而言是可以在目录中做写操作）和可执行（对目录而言是可以访问）三种，分别以 r, w, x 表示，其含义为：对于一个文件来说，可以将用户分成三种，即文件所有者、同组用户、其他用户，可对其分别赋予不同的权限。每一个文件或目录的访问权限都有三组，每组用三位表示，如图 10-8 所示。

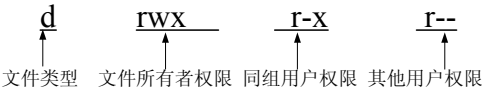


图 10-8 Linux 下对象权限列表图

注：文件类型有多种，d 代表目录，- 代表普通文件，c 代表字符设备文件。

试题 27 答案

(29) B

试题 28 分析

域本地组的成员可以来自森林中的任何域，域本地组用来访问同一域中的资源。在本机模式中的域本地组可以包含森林中任意域内的用户账户、全局组和通用组以及同一域内的域本地组。在混合模式域中，它们能包含任意域中的用户账户和全局组。

试题 28 答案

(30) A

试题 29 分析

SNMPv3 是 SNMP 协议的最新版本, 可以将各个版本的 SNMP 集中在一起工作。SNMP 管理站和代理在 SNMPv3 中被统一称作 SNMP 实体。SNMP 实体由一个 SNMP 引擎和一个或多个 SNMP 应用程序组成。

试题 29 答案

(31) A

试题 30 分析

/etc/shadow 文件用于保存 Linux 系统中用户登录密码信息, 当然是使用加密后的形式。shadow 文件仅对 root 用户可读, 保证了用户口令的安全性。

试题 30 答案

(32) C

网络安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学、数论、信息论等多种学科的综合学科。可以毫不夸张地说，一个企业如果没有相应的安全机制，其信息存储、信息传输都会暴露在外，给黑客软件，计算机病毒入侵，木马植入提供了可乘之机，造成的损失是不可估量的。一套完整、合理的安全机制又是多样化的安全技术、安全类设备、客户的安全意识等多个元素的综合体。

11.1 考点脉络

本章是网络工程师考试的一个必考点，根据考试大纲，要求考生掌握以下几个方面的内容。

- (1) 网络安全基础：对其相关概念了解即可。
- (2) 计算机病毒：主要考查病毒的分类、病毒的攻击方式。
- (3) 加密与密钥管理：主要考查对称加/解密算法、非对称加/解密算法。
- (4) 数字签名与数字证书：主要考查数字签名算法、数字证书格式。
- (5) 入侵检测与防火墙技术：主要考查入侵检测系统、防火墙分类、PIX 防火墙配置命令。
- (6) 电子商务与 VPN：主要考查 SSL、Kerberos、VPN 分类。

从历年的考试试题来看，本章的考点在综合知识考试中的平均分数为 6 分，约为总分的 8%。考试试题分数主要集中在病毒分类、加/解密技术、认证技术、防火墙和 VPN 这 5 个知识点上。

11.2 网络安全基础和计算机病毒

在网络安全基础和计算机病毒这个考点中，主要涉及两个方面的知识，分别是网络安全相关概述、计算机病毒分类和常见攻击手段。

11.2.1 考点精讲

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。网络安全从其本质上来讲就是网络上的信息安全。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全的研究领域。

计算机病毒（Computer Virus）在《中华人民共和国计算机信息系统安全保护条例》中被明确定义，病毒指“编制者在计算机程序中插入的破坏计算机功能或者破坏数据，影响计

算机使用并且能够自我复制的一组计算机指令或者程序代码”。

1. 网络安全基础

本知识点在于让考生理解安全的基本要素、常见的安全威胁与可采取的安全机制，以及常见的安全技术。

(1) 安全的基本要素

信息安全具有以下 5 个基本要素。

- ① 机密性：确保信息不暴露给未授权的实体或进程。
- ② 完整性：只有得到允许的人才能够修改数据，并能够判别数据是否已被篡改。
- ③ 可用性：得到授权的实体在需要时可访问数据。
- ④ 可控性：可以控制授权范围内的信息流向和行为方式。
- ⑤ 可审查性：对出现的安全问题提供调查的依据和手段。

对于网络及网络交易而言，信息安全的基本需求是机密性（又称为保证性）、完整性和不可抵赖性（也就是数据发送、交易发送方无法否认曾经的事实）。

(2) 常见的网络安全威胁

常见的网络安全威胁包括：窃听（即非授权访问、信息泄露、资源盗取等）、假冒（假扮另一个实体，如网站假冒、IP 欺骗等）、重放、流量分析、破坏完整性、拒绝服务、资源的非法授权使用、陷门和特洛伊木马、病毒、诽谤。

另外，对于网络安全而言，大都是针对网络安全漏洞进行网络攻击。其中安全漏洞包括物理安全隐患、软件安全漏洞、搭配的安全漏洞；网络攻击可分为被动攻击、主动攻击、物理临近攻击、内部人员攻击、分发攻击等。

主动攻击和被动攻击的形式如图 11-1 所示。

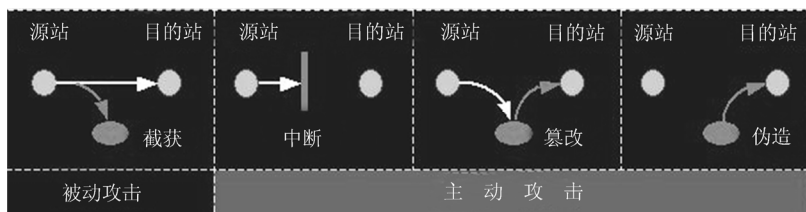


图 11-1 对网络的被动攻击和主动攻击

(3) 安全机制

安全机制可分为两类，一类与安全服务有关，用来实现安全服务；另一类与管理功能有关，用于加强对安全系统的管理。

① 加密机制：可用来加密存放着的数据或流通中的信息，它既可以单独使用，也可以同其他机制结合使用。加密算法一般分为单密钥系统和公开密钥系统。

② 数字签名机制：对信息进行签字的过程，对已签字的信息进行证实的过程。

③ 访问控制机制：根据实体的身份及其有关信息，决定该实体的访问权限。

④ 数据完整性机制：判断在通信过程中信息本体是否被篡改过。在通信中，发送方根据要发送的信息产生一条额外的信息，将后者加密以后随信息本体一同发出；接收方接收到信息本体以后，产生相应的额外信息，并与接收到的额外信息进行比较，以判断在通信过程中信息本体是否被篡改过。

⑤ 认证交换机制：用来实现同级之间的认证，可以使用认证信息，也可以利用实体所具有的特征。

⑥ 防业务流分析机制：通过填充冗余的业务流来防止攻击者进行业务流量分析，填充过的信息要加密保护才能有效。

⑦ 路由控制机制：为了使用安全的子网、中继站和链路，既可预先安排网络中的路由，也可对其动态地进行选择。

⑧ 公证机制：由第三方参与签名机制，基于通信双方对第三方的绝对信任，让公证方备有适用的数字签名、加密或完整性机制。

从 OSI 七层网络结构的角度来看，在物理层可以采用防窃听技术来加强通信线路的安全；在数据链路层可以使用通信保密技术来进行链路加密，使用 L2TP、PPTP 来实现二层隧道通信；在网络层可以采用防火墙来处理信息内外网络边界流动，利用 IPSec 建立透明的安全加密信道；在传输层可以使用 SSL 来将低层安全服务进行抽象和屏蔽；最有效的一类安全机制是可以在传输层和应用层之间建立中间件层次实现通用的安全服务功能，通过定义统一的安全服务接口向应用层提供身份认证、访问控制和数据加密等安全服务。

2. 计算机病毒

本知识点重点在于让考生了解计算机病毒的特点、分类，熟悉常见的几种病毒特征、入侵方式等。

计算机病毒，是指编制或者在计算机程序中插入的破坏计算机的功能或毁坏数据，影响计算机的使用，并能自我复制的一组计算机指令或者程序代码。

（1）病毒的分类

按照计算机病毒的特点及特性，计算机病毒的分类方法有许多种。因此，同一种病毒可能有多种不同的分法，最常见的分类方法是按照寄生方式和传染途径分类。计算机病毒按其寄生方式大致可分为两类，一是引导型病毒，二是文件型病毒；混合型病毒集这两种病毒特性于一体。

① 引导型病毒会去改写（即一般所说的“感染”）磁盘上引导扇区（Boot Sector）的内容（软盘或硬盘都有可能被感染病毒）或者改写硬盘上的分区表（FAT）。如果用已被感染病毒的软盘来启动，则会感染硬盘。

② 文件型病毒主要以感染文件扩展名为 .com、.exe 和 .ovl 等可执行程序为主。它的安装必须借助于病毒的载体程序，即要运行病毒的载体程序，才能把文件型病毒引入内存。已感染病毒的文件执行速度会减缓，甚至完全无法执行。有些文件遭感染后，一执行就会遭到删除。

③ 混合型病毒综合引导型和文件型病毒的特性，它的“性情”比引导型和文件型病毒更为“凶残”。此种病毒通过这两种方式来感染文件，大大提高了病毒的传染性以及存活率。不管以哪种方式传染，只要文件中毒就会经开机或执行程序而感染其他磁盘或文件，此种病毒也是最难杀灭的。

④ 宏病毒是一种寄生于文档或模板（Word 或 Excel）宏中的计算机病毒。一旦打开这样的文档，宏病毒就会被激活，转移到计算机上，并驻留在 Normal 模板上。从此以后，所有自动保存的文档都会“感染”上这种宏病毒，而且如果其他用户打开了感染病毒的文档，宏病毒又会转移到他的计算机上。

(2) 常见的病毒攻击

下面介绍几种常见的病毒攻击行为。

① ARP 欺骗攻击

IP 数据报在局域网内部传输时并不是靠 IP 地址而是靠 MAC 地址来识别目标的，因此 IP 地址与 MAC 地址之间就必须存在一种对应关系。IP 地址与 MAC 对应的关系依靠 ARP 表，每台主机（包括网关）都有一个 ARP 缓存表。在正常情况下，这个缓存表能够有效地保证数据传输的一对一性，也就是说，主机 A 与其他主机（主机 C）之间的通信只通过网关 1，像主机 B 等是无法截获主机 A 与主机 C 之间的通信信息的。但是在 ARP 缓存表的实现机制中存在一个不完善的地方，当主机收到一个 ARP 的应答包后，它并不会去验证自己是否发送过这个 ARP 请求，而是直接将应答包里的 MAC 地址与 IP 对应的关系替换掉原有的 ARP 缓存表里的相应信息，如图 11-2 所示。

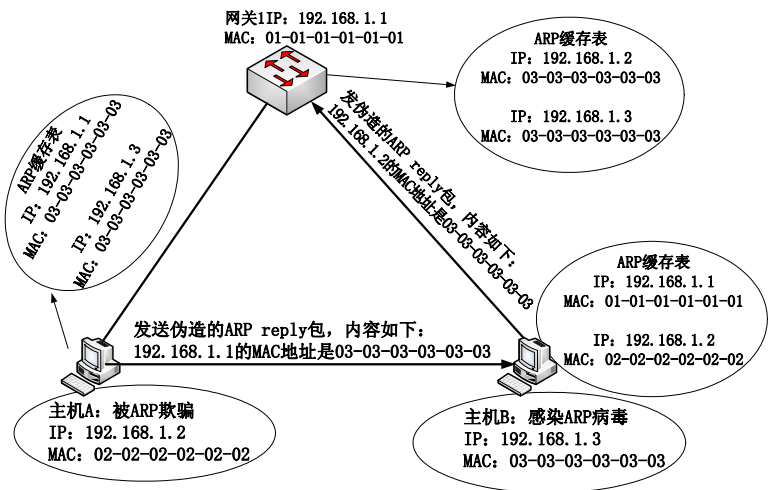


图 11-2 ARP 攻击示意图

这就导致主机 B 截取主机 A 与主机 C 之间的数据通信成为可能。在 ARP 欺骗中，首先主机 B 向主机 A 发送一个 ARP 应答包说 192.168.1.1 的 MAC 地址是 03-03-03-03-03-03，主机 A 收到这个包后并没有去验证包的真实性而是直接将自己 ARP 列表中的 192.168.1.1 的 MAC 地址替换成 03-03-03-03-03-03，同时主机 B 向网关 1 发送一个 ARP 响应包说 192.168.1.2 的 MAC 地址是 03-03-03-03-03-03，同样网关 1 也没有去验证这个包的真实性就把自己 ARP 表中的 192.168.1.2 的 MAC 地址替换成 03-03-03-03-03-03。当主机 A 想要与主机 C 通信时，它直接把应该发送给网关 1（192.168.1.1）的数据报发送到 03-03-03-03-03-03 这个 MAC 地址，也就是发送给了主机 B，主机 B 在收到这个包后经过修改再转发给真正的网关 1，当从主机 C 返回的数据报到达网关 1 后，网关 1 也使用自己 ARP 表中的 MAC 地址，将发往 192.168.1.2 这个 IP 地址的数据发往 03-03-03-03-03-03 这个 MAC 地址，也就是主机 B，主机 B 在收到这个包后再转发给主机 A 完成一次完整的数据通信，这样就成功地实现了一次 ARP 欺骗攻击。

因此，简单地说，ARP 欺骗的目的就是为了实现全交换环境下的数据监听与篡改。到这里我们可以知道要完成一次有效的 ARP 欺骗的关键点就是双向欺骗，也就是说，欺骗者必须同时对网关和主机进行欺骗。

Windows 操作系统带有 ARP 命令程序，可以在 Windows 的命令提示符下使用这个命令来完成 ARP 绑定。ARP 命令及参数如表 11-1 所示。

② 冲击波病毒

该蠕虫病毒利用 RPC 的 DCOM 接口的漏洞，向远端系统上的 RPC 系统服务所监听的端口发送攻击代码，从而达到传播的目的。中毒症状有：计算机莫名其妙地死机或重新启动；IE 浏览器不能正常地打开链接地址；不能复制/粘贴；有时出现应用程序异常的情况；网络变慢；最重要的是，在任务管理器里有一个“msblast.exe”的进程在运行。

表 11-1 ARP 命令及参数

参 数	命 令 格 式	命 令 描 述
-a	arp -a	查看当前主机上的 ARP 映射表。可以看到当前 ARP 的映射关系是动态的还是静态的
-s	arp -s w.x.y.z aa-bb-cc-dd-ee-ff	添加静态的 ARP 实现 ARP 绑定。其中 w.x.y.z 代表要绑定的 IP 地址，aa-bb-cc-dd-ee-ff 代表其 MAC 地址
-d	arp -d InetAddr [IfaceAddr]	删除指定的 IP 地址项，此处的 InetAddr 代表 IP 地址，要删除所有项，应使用星号 (*) 通配符代替

③ 震荡波病毒

震荡波（Worm.Sasser）利用 Windows 平台的 Lsass 漏洞进行传播，中毒后的系统将开启 128 个线程去攻击其他网上的用户。中毒症状：机器运行缓慢、网络堵塞，并让系统不停地进行倒计时重启。其破坏程度有可能超过“冲击波”。

④ 熊猫烧香病毒

熊猫烧香病毒又称“武汉男生”，随后又化身为“金猪报喜”，这是一个感染型蠕虫病毒，能感染系统中.exe、.com、.pif、.src、.html、.asp 等文件，还能中止大量的反病毒软件进程并且会删除扩展名为.gho 的文件，被感染的用户系统中所有.exe 可执行文件图标全部被改成熊猫举着三根香的模样。

⑤ DoS（拒绝服务）与 DDoS

最基本的 DoS 攻击就是利用合理的服务请求来占用过多的服务资源，致使服务超载，无法响应其他的请求。这些服务资源包括网络带宽、文件系统空间容量、开放的进程或者向内的连接。这种攻击会导致资源的匮乏，无论计算机的处理速度多么快，内存容量多么大，互联网的速度多么快都无法避免这种攻击带来的后果。因为任何事情都有一个极限，所以，总能找到一个方法使请求的值大于该极限值，因此就会使所提供的服务资源匮乏。千万不要自认为拥有了足够宽的带宽就会有一个高效率的网站，拒绝服务攻击会使所有的资源变得非常渺小。

DDoS 攻击手段是在传统的 DoS 攻击基础之上产生的一类攻击方式。一个比较完善的 DDoS 攻击体系分成 4 大部分，最重要的是第 2 部分和第 3 部分：它们分别用做控制攻击和实际发起的攻击。请注意控制机与攻击的区别，对第 4 部分的受害者来说，DDoS 的实际攻击包是从第 3 部分攻击机上发出的，第 2 部分的控制机只发布命令而不参与实际的攻击。对第 2 部分和第 3 部分计算机，黑客有控制权或者部分的控制权，并把相应的 DDoS 程序上传到这些平台上，这些程序与正常的程序一样运行并等待来自黑客的指令，通常它还会利用各种手段隐藏自己不被别人发现。在平时，这些傀儡机器并没有什么异常，只是一旦黑客连接到它们，并发出控制指令的时候，攻击傀儡机就成为攻击源向受害者发起攻击。

11.2.2 一点一练

试题 1

以下关于钓鱼网站的说法中，错误的是____（1）_____。

- (1) A. 钓鱼网站仿冒真实网站的 URL 地址
- B. 钓鱼网站是一种网络游戏
- C. 钓鱼网站用于窃取访问者的机密信息
- D. 钓鱼网站可以通过 E-mail 传播网址

试题 2

在网络管理中要防止各种安全威胁。在 SNMP 中, 无法预防的安全威胁是__(2)___。

- (2) A. 篡改管理信息: 通过改变传输中的 SNMP 报文实施未经授权的管理操作
- B. 通信分析: 第三者分析管理实体之间的通信规律, 从而获取管理信息
- C. 假冒合法用户: 未经授权的用户冒充授权用户, 企图实施管理操作
- D. 消息泄露: SNMP 引擎之间交换的信息被第三者偷听

试题 3

下面病毒中, 属于蠕虫病毒的是__(3)___

- (3) A. Worm.Sasser 病毒
- B. Trojan.QQPSW 病毒
- C. Backdoor.IRCBot 病毒
- D. Macro.Melissa 病毒

试题 4

杀毒软件报告发现病毒 Macro.Melissa, 由该病毒名称可以推断出病毒的类型是__(4)___, 这类病毒主要感染目标是__(5)___。

- (4) A. 文件型
- B. 引导型
- C. 目录型
- D. 宏病毒
- (5) A. EXE 或 COM 可执行文件
- B. Word 或 Excel 文件
- C. DLL 系统文件
- D. 磁盘引导区

试题 5

在下面 4 种病毒中, __(6)___ 可以远程控制网络中的计算机。

- (6) A. worm.Sasser.f
- B. Win32.CIH
- C. Trojan.qq3344
- D. Macro.Melissa

11.2.3 解析与答案

试题 1 分析

所谓“钓鱼网站”是一种网络欺诈行为, 指不法分子利用各种手段, 仿冒真实网站的 URL 地址以及页面内容, 或者利用真实网站服务器程序上的漏洞在站点的某些网页中插入危险的 HTML 代码, 以此来骗取用户银行或信用卡的账号、密码等私人资料。

试题 1 答案

- (1) B

试题 2 分析

在网络管理中要防止各种安全威胁。安全威胁分为主要和次要两类, 其中主要的威胁有以下两种。

- ① 篡改管理信息: 通过改变传输中的 SNMP 报文实施未经授权的管理操作。
- ② 假冒合法用户: 未经授权的用户冒充授权用户。

企图实施管理操作次要的威胁有以下两种。

- ① 消息泄露: SNMP 引擎之间交换的信息被第三者偷听。
- ② 修改报文流: 由于 SNMP 协议通常是基于无连接的传输服务, 重新排序报文流、延迟或重放报文的威胁都可能出现。这种威胁的危害性在于通过报文流的修改可能实施非法的管理操作。

另外有两种威胁是安全体系结构不必防护的, 因为不重要或者是无法预防的。

① 拒绝服务：因为很多情况下拒绝服务和网络失效是无法区别的，所以可以由网络管理协议来处理，安全系统不必采取措施。

② 通信分析：第三者分析管理实体之间的通信规律，从而获取管理信息。

试题 2 答案

(2) B

试题 3 分析

病毒的命名规则：一般格式为<病毒前缀>.<病毒名>.<病毒后缀>，病毒前缀是指一个病毒的种类，它是用来区别病毒的种族分类的。不同种类的病毒，其前缀也是不同的。例如，我们常见的木马病毒的前缀是 Trojan，蠕虫病毒的前缀是 Worm 等。

试题 3 答案

(3) A

试题 4 分析

为了方便管理各种计算机病毒，通常按照病毒的特性，将病毒进行分类命名。通常的格式如下：

<病毒前缀>.<病毒名>.<病毒后缀>

病毒前缀是指一个病毒的种类，用来区别病毒的种族分类的。不同种类的病毒，其前缀也是不同的。例如，常见的木马病毒的前缀 Trojan，蠕虫病毒的前缀是 Worm，宏病毒用 Macro。

病毒名是指一个病毒的家族特征，是用来区别和标识病毒家族的，如以前著名的 CIH 病毒的家族名都是统一的 CIH，震荡波蠕虫病毒的家族名是 Sasser 等。

病毒后缀是指一个病毒的变种特征，是用来区别具体某个家族病毒的某个变种的。一般都采用英文中的 26 个字母来表示，如 Worm.Sasser.b 就是指振荡波蠕虫病毒的变种 B，因此一般称为“震荡波 B 变种”或者“震荡波变种 B”。

宏病毒主要是感染 Microsoft 的 Office 系统文件。

试题 4 答案

(4) D

(5) B

试题 5 分析

本题考查病毒的相关知识。

在选项中的 4 种病毒中，worm 是蠕虫病毒，Win32.CIH 是 CIH 病毒，Macro.Melissa 是宏病毒，这三种病毒都属于单机病毒；而 Trojan.qq3344 是一种特洛伊木马，通过网络实现对计算机的远程攻击。

试题 5 答案

(6) C

11.3 加解密技术和认证技术

在加/解密技术和认证技术这个考点中，主要涉及三个方面的知识，分别是加/解密算法、数字签名和数字证书。

11.3.1 考点精讲

加/解密算法主要分为共享密钥加密（对称加密）和公共密钥加密（非对称加密）。

身份认证技术是在计算机网络中确认操作者身份的过程而产生的解决方法。计算机网

络世界中一切信息包括用户的身份信息都是用一组特定的数据来表示的,计算机只能识别用户的数字身份,所有对用户的授权也是针对用户数字身份的授权。如何保证以数字身份进行操作的操作者就是这个数字身份的合法拥有者,也就是说保证操作者的物理身份与数字身份相对应,身份认证技术就是解决这个问题的。作为防护网络资产的第一道关口,身份认证有着举足轻重的作用。数字签名和数字证书都起到身份认证的作用。

1. 加密和解密技术

本知识点主要是让考生掌握对称密钥技术和非对称密钥技术的区别与主要特征,了解对称密钥技术的代表 DES、3DES、IDEA 以及非对称密钥技术的代表 RSA 的主要技术特征,特别要注意 RSA 算法。

(1) 对称密钥技术

对称密钥技术是指加密系统的加密密钥和解密密钥相同,或者两者虽然不同,但通过其中的任意一个可以很容易地推导出另一个。其优点是具有很高的保密强度,但密钥的传输需要经过安全可靠的途径。

对称密钥技术有两种基本类型:分组密码(它是在明文分组和密文分组上进行运算的)和序列密码(对明文和密文数据流按位或字节进行运算)。常见的对称密钥技术包括以下两种。

① 它是一种迭代的分组密码,输入/输出都是 64 位,使用一个 56 位的密钥以及附加的 8 位奇偶校验位,有弱钥,但可避免。攻击 DES 的主要技术是穷举。但由于 DES 的密钥长度较短,因此为了提高安全性,就出现了使用 112 位密钥对数据进行三次加密的算法,即 3DES。

② IDEA 算法:其明文和密文都是 64 位,密钥长度为 128 位。

(2) 非对称密钥技术

非对称密钥技术也称为公钥算法,就是指加密系统的加密密钥和解密密钥完全不同,并且不可能从任何一个推导出另一个。它的优点在于可以适应开放性的使用环境,可以实现数字签名与验证。

最常见的非对称密钥技术就是 RSA,其理论基础是数论中大素数分解。但如果使用 RSA 来加密大量的数据,则速度太慢,效率不高,因此 RSA 广泛用于密钥的分发(对会话密钥进行加密)。公开密钥算法现在主要包括两大类算法:建立在基于“分解大素数的困难度”基础上的算法,和建立在“以大素数为模来计算离散对数的困难度”基础上的算法。

2. 密钥管理机制

本知识点重点在于让考生理解密钥管理的作用,了解 KMI、PKI、SPK 的技术与应用特点即可,不需作过多的理解。

密钥管理是指处理密钥自产生到销毁整个过程中的有关问题,包括系统的初始化,密钥的产生、存储、备份/恢复、装入、分配、保护、更新、控制、丢失、吊销及销毁。当前主要的密钥管理体制有三种:适用于封闭网、以传统的密钥管理中心为代表的 KMI 机制;适用于开放网的 PKI 机制;适用于规模化专用网的 SPK 机制。

(1) KMI 机制

KMI 机制分发密钥的安全性依赖于秘密信道,见表 11-2。

表 11-2 密钥分发机制

分发类型	技术	特点
静态分发	点对点配置	可用单钥或双钥实现。单钥为鉴别提供可靠参数，但不提供不可否认服务。数字签名要求双钥实现
	一对多配置	可用单钥或双钥实现。只在中心保留所有各端的密钥，各端只保留自己的密钥。是建立秘密通道的主要办法
	格状网配置	可用单钥或双钥实现。也称为端端密钥，密钥配置量为全网 n 个终端中选 2 的组合数
动态分发	基于单钥的单钥分发	首先用静态分发方式配置星状密钥，主要解决会话密钥的分发
	基于单钥的双钥分发	公钥私钥对都当作秘密变量

(2) PKI 机制

PKI 机制解决了分发密钥时依赖秘密信道的问题，PKI 与 KMI 比较见表 11-3。

表 11-3 PKI 与 KMI 比较

项 目	PKI	KMI
作用特性	良好的扩展性，适于开放业务	很好的封闭性，适用于专用业务
服务功能	只提供数字签名服务	提供加密和签名功能
信任逻辑	第三方管理模式	集中式的主管方管理模式
负责性	个人负责的技术体系	单位负责制
应用角度	主外	主内

(3) SPK 机制

为了更好地解决密钥管理的问题，现在提出了种子化公钥 (SPK) 和种子化双钥 (SDK) 体系。在 SPK 体制中可以实现以下两种公钥。

① 多重公钥 (双钥)，即 LPK/LDK，用 RSA 公钥算法实现。

② 组合公钥 (双钥)，即 CPK/CDK，用离散对数 DLP 或椭圆曲线密码 ECC 实现。它是电子商务和电子政务中比较理想的密钥解决方案。

3. 数字签名

认证技术主要解决网络通信过程中通信双方的身份认证。认证的过程涉及加密和密钥交换。通常，加密可使用对称加密、非对称加密及两种加密方法混合的方法。认证方一般有账户名/口令认证、使用摘要算法认证、基于 PKI 的认证。

(1) Hash 函数和信息摘要

Hash 函数又称为杂凑函数、散列函数，它提供的计算过程为：输入一个长度不固定的字符串，返回一串定长的字符串 (又称为 Hash 值)。单向 Hash 函数用于产生信息摘要。

信息摘要简要地描述了一份较长的信息或文件，它可以被看做是一份长文件的数字指纹，信息摘要可以用于创建数字签名。对于特定的文件而言，信息摘要是唯一的，而且不同的文件必将产生不同的信息摘要。常见的信息摘要算法包括 MD5 (产生一个 128 位的输出，输入是以 512 位的分组进行处理的) 和 SHA (安全散列算法，也是按 512 位的分组进行处理，产生一个 160 位的输出)，它们可以用来保护数据的完整性。

(2) 数字签名技术

数字签名是通过一个单向函数对要传送的报文进行处理得到用以认证报文来源并核实

报文是否发生变化的一个字母数字串。它与数据加密技术一起构建起了安全的商业加密体系：传统的数据加密是保护数据的最基本方法，它只能够防止第三者获得真实的数据（即数据的机密性）；而数字签名则可以解决否认、伪造、篡改和冒充的问题（即数据的完整性和不可抵赖性）。

数字签名可以使用对称加密技术实现，也可以使用非对称加密技术（公钥算法）实现。但使用对称加密技术实现，需要第三方认证，比较麻烦。因此现在通常使用的是公钥算法。

整个数字签名应用过程很简单，具体介绍如下。

① 信息发送者使用一个单向散列函数对信息生成信息摘要。

② 信息发送者使用自己的私钥签名信息摘要。

③ 信息发送者把信息本身和已签名的信息摘要一起发送出去。

④ 信息接收者通过使用与信息发送者使用的同一个单向散列函数对接收的信息本身生成新的信息摘要，再使用信息发送者的公钥对信息摘要进行验证，以确认信息发送者的身份是否被修改过。

如果接收者收到的信息是 P（用 E 代表公钥，D 代表私钥），那么要保留的证据就应该是 E 发送者（P），这也就证明了信息的确是“发送者”发出的。

4. 数字证书

数字证书采用公钥体制，即利用一对互相匹配的密钥进行加密和解密。每个用户将设定一个私钥（仅为本人所知的专用密钥，用来解密和签名）和一个公钥（由本人公开，用于加密和验证签名），用以实现：

① 发送机密文件。发送方使用接收方的公钥进行加密，接收方便使用自己的私钥解密。

② 接收方能够通过数字证书来确认发送方的身份，发送方无法抵赖。

③ 信息自数字签名后可以保证信息无法更改。

（1）数字证书的格式

数字证书的格式一般使用 X.509 国际标准。X.509 是广泛使用的证书格式之一，X.509 用户公钥证书是由可信赖的证书权威机构（CA——证书授权中心）创建的，并且由 CA 或用户存放在 X.500 的目录中。

在 X.509 格式中，数字证书通常包括：版本号、序列号（CA 下发的每个证书的序列号都是唯一的）、签名算法标识符、发行者名称、有效性、主体名称、主体的公开密钥信息、发行者唯一识别符、主体唯一识别符、扩充域、签名（就是 CA 用自己的私钥对上述域进行数字签名的结果，也可以理解为是 CA 中心对用户证书的签名）。

（2）数字证书的获取

任何一个用户只要得到 CA 中心的公钥，就可以得到该 CA 中心为该用户签署的公钥。因为证书是不可伪造的，因此对于存放证书的目录无须施加特别的保护。

因为用户数量众多，因此会存在多个 CA 中心。但如果两个用户使用的是不同 CA 中心发放的证书，则无法直接使用证书；但如果两个证书发放机构之间已经安全地交换了公开密钥，则可以使用证书链来完成通信。

（3）证书的吊销

证书到了有效期、用户私钥已被泄露、用户放弃使用原 CA 中心的服务、CA 中心私钥泄露时都需要吊销证书，这时 CA 中心会维护一个证书吊销列表 CRL，供大家查询。

11.3.2 一点一练

试题 1

甲和乙要进行通信,甲对发送的消息附加了数字签名,乙收到该消息后利用____(1)____验证该消息的真实性。

- (1) A. 甲的公钥 B. 甲的私钥 C. 乙的公钥 D. 乙的私钥

试题 2

下列算法中,____(2)____属于摘要算法。

- (2) A. DES B. MD5 C. Diffie-Hellman D. AES

试题 3

公钥体系中,用户甲发送给用户乙的数据要用____(3)____进行加密。

- (3) A. 甲的公钥 B. 甲的私钥 C. 乙的公钥 D. 乙的私钥

试题 4

下列选项中,同属于报文摘要算法的是____(4)____。

- (4) A. DES 和 MD5 B. MD5 和 SHA-1 C. RSA 和 SHA-1 D. DES 和 RSA

试题 5

如图 11-3 所示为一种数字签名方案,网上传送的报文是____(5)____,防止 A 抵赖的证据是____(6)____。

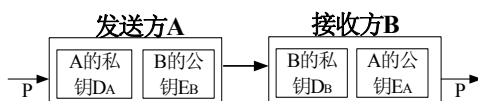


图 11-3 数字签名方案

- (5) A. P B. DA (P) C. EB (DA (P)) D. DA
(6) A. P B. DA (P) C. EB (DA (P)) D. DA

11.3.3 解析与答案

试题 1 分析

数字签名 (Digital Signature) 技术是不对称加密算法的典型应用。数字签名的应用过程是,数据源发送方使用自己的私钥对数据校验或其他与数据内容有关的变量进行加密处理,完成对数据的合法“签名”,数据接收方则利用对方的公钥来解读收到的“数字签名”,并将解读结果用于对数据完整性的检验,以确认签名的合法性。

试题 1 答案

- (1) A

试题 2 分析

DES 算法为美国数据加密标准,是 1972 年美国 IBM 公司研制的对称密码体制加密算法。Diffie-Hellman 为密钥交换算法。高级加密标准 AES,是美国联邦政府采用的一种区块加密标准。这个标准用来替代原先的 DES 加密算法。报文摘要是指单向哈希函数算法将任意长度的输入报文经计算得出固定位的输出。所谓单向是指该算法是不可逆的,找出具有同一报文摘要的两个不同报文是很困难的,常见的报文摘要算法有 MD5、SHA。

试题 2 答案

- (2) B

试题 3 分析

在公钥密码体系中，加密密钥是公开的，而解密密钥是需要保密的。在公钥密码体系中，密钥对产生器产生出接收者乙的一对密钥：加密密钥和解密密钥。发送者甲所用的加密密钥就是接收者乙的公钥，向公众公开。而乙所用的解密密钥就是接收者的私钥，对其他人保密。

试题 3 答案

(3) C

试题 4 分析

报文摘要算法 (Message Digest Algorithms) 即采用单向 HASH 算法将需要加密的明文进行摘要，而产生的具有固定长度的单向散列 (HASH) 值。其中，散列函数 (Hash Functions) 是将一个不同长度的报文转换成一个数字串 (即报文摘要) 的公式，该函数不需要密钥，公式决定了报文摘要的长度。报文摘要和非对称加密一起，提供数字签名的方法。报文摘要算法主要有安全散列标准 SHA-1、MD5 系列标准。

试题 4 答案

(4) B

试题 5 分析

报文的发送方用一个哈希函数从报文文本中生成报文摘要 (散列值)。发送方用自己的私人密钥对这个散列值进行加密。然后，这个加密后的散列值将作为报文的附件和报文一起发送给报文的接收方。报文的接收方首先用与发送方一样的哈希函数从接收到的原始报文中计算出报文摘要，接着再用发送方的公用密钥来对报文附加的数字签名进行解密。如果两个散列值相同，那么接收方就能确认该数字签名是发送方的。通过数字签名能够实现对原始报文的鉴别。

试题 5 答案

(5) C

(6) B

11.4 入侵检测系统与防火墙技术

在入侵检测系统和防火墙技术这个考点中，主要涉及三个方面的知识，分别是入侵检测系统的构成、防火墙分类和 PIX 防火墙配置。

11.4.1 考点精讲

入侵检测 (Intrusion Detection) 是对入侵行为的检测。它通过收集和分析网络行为、安全日志、审计数据、其他在网络上可以获得的信息以及计算机系统中若干关键点的信息，检查网络或系统中是否存在违反安全策略的行为和被攻击的迹象。入侵检测作为一种积极主动的安全防护技术，提供了对内部攻击、外部攻击和误操作的实时保护，在网络系统受到危害之前拦截和响应入侵，因此被认为是防火墙之后的第二道安全闸门。

顾名思义，防火墙就是用来阻挡外部不安全因素影响的内部网络屏障，其目的就是防止外部网络用户未经授权的访问。它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关 (Security Gateway)，从而保护内部网免受非法用户的侵入。如微软公司的 ISA 软件防火墙、思科 PIX 和 ASA 硬件防火墙、北京天融信硬件防火墙都是当前有名的软硬件防火墙。

1. 入侵检测系统

本知识点在于了解入侵检测技术的基本概念、本质内容、系统基本结构，以及常见的入

入侵检测方法。

入侵检测技术的核心包括两个方面：一是如何充分并可靠地提取描述行为的特征数据；二是如何根据特征数据，高效并准确地判断行为的性质。入侵检测系统通过从计算机网络或计算机系统的关键点收集信息并进行分析，从中发现网络或系统中是否有违反安全策略的行为和被攻击的迹象。

入侵检测系统的实现过程如图 11-4 所示。

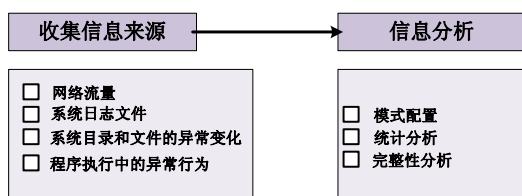


图 11-4 入侵检测系统的实现过程

（1）入侵检测系统的构成

IETF 将一个入侵检测系统分为 4 个组件：事件产生器（Event Generators）、事件分析器（Event Analyzers）、响应单元（Response Units）和事件数据库（Event Databases）。

① 事件产生器的目的是从整个计算环境中获得事件，并向系统的其他部分提供此事件。

② 事件分析器分析得到的数据，并产生分析结果。

③ 响应单元则是对分析结果做出反应的功能单元，它可以做出切断连接、改变文件属性等强烈反应，也可以只是简单地报警。

④ 事件数据库是存放各种中间数据和最终数据地方的统称，它可以是复杂的数据库，也可以是简单的文本文件。

（2）入侵检测系统分类

入侵检测系统可以分为 4 类，分别是基于主机、基于网络、基于内核和基于应用的入侵检测系统。

① 基于主机：安全操作系统必须具备一定的审计功能，并记录相应的安全性日志。

② 基于网络：IDS 可以放在防火墙或者网关的后面，以网络嗅探器的形式捕获所有的对内对外的数据报。

③ 基于内核：从操作系统的内核接收数据，如 LIDS。

④ 基于应用：从正在运行的应用程序中收集数据。

（3）入侵检测系统技术

目前，入侵检测技术主要有异常检测和误用检测。

① 异常检测：也称为基于行为的检测。首先建立起用户的正常使用模式，即知识库，标识出不符合正常模式的行为活动。

② 误用检测：也称为基于特征的检测。首先建立起已知攻击的知识库，判别当前行为活动是否符合已知的攻击模式。

2. 防火墙技术

本节重点在于让考生理解防火墙的基本概念、类别，掌握防火墙的常见结构以及 PIX 防火墙的相关配置。

(1) 防火墙基础

防火墙一般分为两类。

① 网络级防火墙：用来防止整个网络出现外来非法的入侵。属于这类的防火墙有分组过滤和授权服务器。前者检查所有流入本网络的信息，然后拒绝不符合事先制定好的一套准则的数据；而后者则是检查用户的登录是否合法。

② 应用级防火墙：从应用程序来进行接入控制。通常使用应用网关或代理服务器来区分各种应用。例如，可以只允许访问万维网的应用通过，而阻止 FTP 应用的通过。

根据不同的应用，对防火墙进行了详细划分，参见表 11-4。

表 11-4 防火墙分类

类 型	特 点	优 点	缺 点
包过滤 (访问控制表)	根据定义的过滤规则审查， 根据是否匹配来决定是否通过	透明、成本低、 速度快、效率高	对 IP 包伪造难以防范，不具备身份认证功能，不能检测高层攻击，过滤多，效率下降快
应用网关	工作在应用层，实现协议过滤和转发功能	能够提供比较成熟的日志功能	速度相对更慢
代理服务	阻断内外网之间的通信，只能够通过“代理”实现	有很高的安全性	速度慢，对用户不透明，协议不同就需要不同的代理，不利于网络新业务
状态检测 (自适应/动态包过滤)	通过状态检测技术动态记录、维护各个连接的协议状态	效率很高，动态修改规则可以提高安全性	所有这些记录、测试和分析工作可能会造成网络连接的某种迟滞，特别是在同时有许多连接被激活时，或者有大量的过滤网络通信的规则存在时
自适应代理	根据用户的安全策略，动态适应传输中的分组流量	状态检测+代理	速度相对比较慢，当用户对内外网网络网关的吞吐量要求比较高时，代理防火墙就会成为内外网网络之间的瓶颈，给系统性能带来了一些负面影响，但通常不会很明显

防火墙的功能有两个：阻止和允许。“阻止”就是阻止某种类型的通信量通过防火墙（从外部网络到内部网络，或反过来）。“允许”功能与“阻止”功能恰好相反，防火墙必须能够识别通信量的各种类型。不过，在大多数情况下防火墙的主要功能是“阻止”。

(2) 常见的防火墙技术

防火墙的种类多种多样，在不同的发展阶段，采用的技术也各不相同，因而也就产生了不同类型的防火墙。防火墙所采用的技术主要有如下 5 种。

① 屏蔽路由技术

最简单和最流行的防火墙形式是“屏蔽路由器”，采用包过滤或虚电路技术。包过滤通过检查每个 IP 网络包，取得其头信息，一般包括：到达的物理网络接口，源 IP 地址，目标 IP 地址，传输层类型（TCP、UDP、ICMP），源端口和目的端口。根据这些信息，判别是否与规则集中的某条目匹配，并对匹配包执行规则中指定的动作（禁止或允许）。

② 基于代理的技术

基于代理的防火墙也称应用网关，通常被配置为“双宿主网关”，具有两个网络接口卡，同时接入内部网和外部网。由于网关可以与两个网络通信，它是安装传递数据软件的理想位置。代理服务不允许直接与真正的服务通信，而是与代理服务器通信（用户的默认网关指向

代理服务器)。各个应用代理在用户和服务器之间处理所有的通信，能够对通过它的数据进行详细的审计追踪，许多专家也认为它更加安全，因为代理软件可以根据防火墙后面主机的脆弱性来制定，以专门防范已知的攻击。

③ 过滤技术

系统按照一定的信息过滤规则，对进出内部网络的信息进行限制，允许授权信息通过，而拒绝非授权信息通过。包过滤防火墙工作在网络层和逻辑链路层之间，截获所有流经的 IP 包，从其 IP 头、传输层协议头，甚至应用层协议数据中获取过滤所需的相关信息。然后依次按顺序与事先设定的访问控制规则进行一一匹配比较，执行其相关的动作。

④ 动态防火墙技术

它是针对静态包过滤技术而提出的一项新技术。静态包过滤技术局限于过滤基于源及目的端口，IP 地址的输入/输出业务，因而限制了控制能力。而动态防火墙技术可创建动态的规则，使其适应不断改变的网络业务量。具体地讲，动态防火墙技术并不是根据状态来对包进行有效性检查的，而是通过为每个会话维护其状态信息，来提供一种防御措施和方法。

⑤ DMZ 模型

DMZ 称为“隔离区”，也称为“非军事化区”，它是为了解决安装防火墙后外部网络不能访问内部网络服务器的问题，而设立的一个非安全系统与安全系统之间的缓冲区。这个缓冲区位于企业内部网络和外部网络之间的小网络区域内，在这个小网络区域内可以放置一些必须公开的服务器设施，如企业 Web 服务器、FTP 服务器和论坛等。另外，通过这样一个 DMZ 区域，更加有效地保护了内部网络，因为这种网络部署，比起一般的防火墙方案，对攻击者来说又多了一道关卡。DMZ 模型如图 11-5 所示。

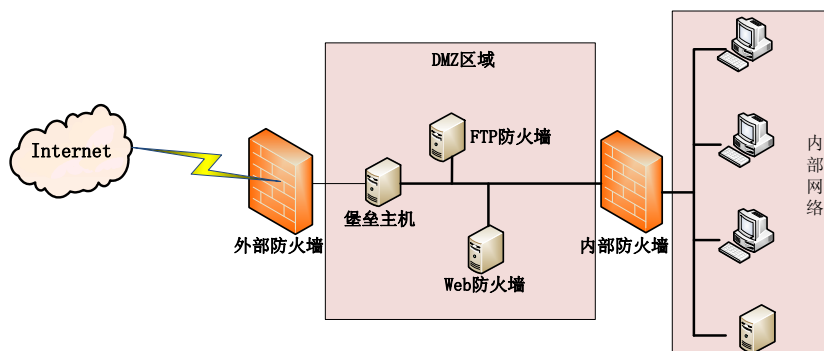


图 11-5 DMZ 模型

在这个防火墙方案中，包括两个防火墙：外部防火墙抵挡外部网络的攻击，并管理所有内部网络对 DMZ 的访问；内部防火墙管理 DMZ 对于内部网络的访问。内部防火墙是内部网络的第三道安全防线（前面有了外部防火墙和堡垒主机），当外部防火墙失效时，它还可以起到保护内部网络的作用。而在局域网内部，对于 Internet 的访问由内部防火墙和位于 DMZ 的堡垒主机控制。

（3）防火墙应用配置

本知识点重点在于让考生了解 Cisco 防火墙的基本配置方法，了解其最基本的指令。在历年考题中还没有出现过直接相关的题目。

硬件防火墙通常在使用时也要进行初始配置，下面就以 Cisco PIX 防火墙为例，说明其配置的关键要点。

① 配置方式：与交换机、路由器都十分接近，包括初始配置必须使用的控制端口连接方式，如通过 Telnet 方式，通过 FTP 服务器软件方式（图形化配置界面）。

② 配置模式：与交换机、路由器十分类似，如表 11-5 所示。

表 11-5 防火墙工作模式

防 火 墙	路由器、交换机	命 令
普通模式	用户模式	无，启动后进入
特权模式	特权模式	enable
配置模式	全局配置模式	config terminal
接口模式	子配置模式	interface 接口名

③ 主要配置项，如表 11-6 所示。

表 11-6 防火墙配置

项 目	命 令 实 例
配置防火墙网卡参数	interface 接口名参数 例：interface ethernet0 auto 将第一个网口设置为自适应网卡
配置内、外部网卡 IP	IP address [inside outside] ip-addr netmask inside 代表内部网卡，outside 代表外部网卡 ip-addr 是指 IP 地址，netmask 是子网掩码
指定外部网卡 IP 地址范围	global 1 ip_addr - ip_addr 两个 ip-addr 参数用来限定 IP 地址范围
指定要进行转换的内部地址	nat 1 ip_addr netmask
配置某些控制选项	conduit global_ip port[-port] protocol foreign_ip netmask global_ip 表示要控制地址；port 表示所作用的端口，0 表示所有端口；protocol 代表连接协议，如 TCP、UPD；foreign_ip 表示可以访问 global_ip 外部 IP 地址；netmask 为可选项

最后可以使用 wr mem 命令将配置的内容保存生效。

11.4.2 一点一练

试题 1

包过滤防火墙对通过防火墙的数据包进行检查，只有满足条件的数据包才能通过，对数据包的检查内容一般不包括____（1）_____。

- (1) A. 源地址 B. 目的地址 C. 协议 D. 有效载荷

试题 2

包过滤防火墙通过____（2）_____来确定数据包是否能通过。

- (2) A. 路由表 B. ARP 表 C. NAT 表 D. 过滤规则

试题 3

____（3）_____不属于将入侵检测系统部署在 DMZ 中的优点。

- (3) A. 可以查看受保护区域主机被攻击的状态
B. 可以检测防火墙系统的策略配置是否合理
C. 可以检测 DMZ 被黑客攻击的重点
D. 可以审计来自 Internet 上对受保护网络的攻击类型

试题 4

公司面临的网络攻击来自多方面，一般通过安装防火墙来防范____(4)____。

(4) A. 外部攻击 B. 内部攻击 C. 网络监听 D. 病毒入侵

试题 5

公司面临的网络攻击来自多方面，安装用户认证系统来防范____(5)____。

(5) A. 外部攻击 B. 内部攻击 C. 网络监听 D. 病毒入侵

11.4.3 解析与答案

试题 1 分析

本题考查包过滤防火墙的相关知识。

防火墙的基本功能是包过滤，能对进出防火墙的数据包包头（包括源地址、目的地址和协议）进行分析处理，但对于数据包的有效载荷一般无法分析处理。所以答案是 D。

试题 1 答案

(1) D

试题 2 分析

包过滤型防火墙工作在 OSI 网络参考模型的网络层和传输层，它根据数据包头源地址、目的地址、端口号和协议类型等标志确定是否允许通过。只有满足过滤条件的数据包才被转发到相应的目的地，其余数据包则被从数据流中丢弃。

包过滤方式是一种通用、廉价和有效的安全手段。之所以通用，是因为它不是针对各个具体的网络服务采取特殊的处理方式，适用于所有网络服务；之所以廉价，是因为大多数路由器都提供数据包过滤功能，所以这类防火墙大多数是由路由器集成的；之所以有效，是因为它在很大程度上满足了绝大多数企业的安全要求。

在整个防火墙技术的发展过程中，包过滤技术出现了两种不同的版本，称为“第一代静态包过滤”和“第二代动态包过滤”。

① 第一代静态包过滤类型防火墙

这类防火墙几乎是与路由器同时产生的，它是根据定义好的过滤规则审查每个数据包，以便确定其是否与某一条包过滤规则匹配。过滤规则基于数据包的报头信息进行制订。报头信息中包括 IP 源地址、IP 目标地址、传输协议（如 TCP，UDP 和 ICMP 等）、TCP/UDP 目标端口和 ICMP 消息类型等。

② 第二代动态包过滤类型防火墙

这类防火墙采用动态设置包过滤规则的方法，避免了静态包过滤所具有的问题。这种技术后来发展成为包状态监测（Stateful Inspection）技术。采用这种技术的防火墙对通过其建立的每一个连接都进行跟踪，并且根据需要可动态地在过滤规则中增加或更新条目。

包过滤方式的优点是不用改动客户机和主机上的应用程序，因为它工作在网络层和传输层，与应用层无关。但其弱点也是明显的：过滤判别的依据只是网络层和传输层的有限信息，因而各种安全要求不可能充分满足；在许多过滤器中，过滤规则的数目是有限制的，且随着规则数目的增加，性能会受到很大的影响；由于缺少上下文关联信息，不能有效地过滤如 UDP、RPC（远程过程调用）一类的协议。另外，大多数过滤器中缺少审计和报警机制，它只能依据包头信息，而不能对用户身份进行验证，很容易受到“地址欺骗型”攻击。其对安全管理人员素质要求高，建立安全规则时，必须对协议本身及其在不同应用程序中的作用有较深入的理解。因此，过滤器通常是和应用网关配合使用，共同组成防火墙系统。

试题 2 答案

(2) D

试题 3 分析

本题考查的是入侵检测系统的配置方面的知识。

入侵检测系统可以配置在防火墙非军事区 (DMZ) 内也可以部署在其外。如果入侵检测系统部署在 DMZ 外, 那么它将不能访问受保护区域主机, 也就无法审计来自 Internet 上的网络攻击。而将入侵检测系统部署在 DMZ 内, 那么入侵检测系统既可以审计来自 Internet 上的网络攻击, 同时还可以检查 DMZ 内设备的状态信息。

试题 3 答案

(3) D

试题 4 分析

防火墙通常是运行在一台或者多台计算机上的一组特别的服务软件, 用于对网络进行防护和通信控制。防火墙隔离了内部网络和外部网络, 所有进出被保护网络的通信数据流必须经过防火墙, 所有通过防火墙的通信必须经过安全策略的过滤或者防火墙的授权。

试题 4 答案

(4) A

试题 5 分析

企业安装用户认证系统是为了防范内部攻击。

试题 5 答案

(5) B

11.5 电子商务与 VPN 技术

在电子商务与 VPN 技术这个考点中, 主要涉及两个方面的知识, 分别是电子商务相关协议介绍和 VPN 分类。

11.5.1 考点精讲

电子商务通常是指在全球各地广泛的商业贸易活动中, 在因特网开放的网络环境下, 基于浏览器/服务器应用方式, 买卖双方不谋面地进行各种商贸活动, 实现消费者的网上购物、商户之间的网上交易和在线电子支付以及各种商务活动、交易活动、金融活动和相关的综合服务活动的一种新型的商业运营模式。电子商务是利用微电脑技术和网络通信技术进行的商务活动。与之相关联的所有安全内容, 可以被称为电子商务安全, 其固然会涉及一些安全的协议和认证技术, 在下面会有详细解说。

虚拟专用网络 (Virtual Private Network, VPN) 指的是在公用网络上建立专用网络的技术。因为整个 VPN 网络的任意两个节点之间的连接并没有传统专网所需的端到端的物理链路, 所以 VPN 是架构在公用网络服务商所提供的网络平台, 如 Internet、ATM (异步传输模式)、Frame Relay (帧中继) 等之上的逻辑网络, 用户数据在逻辑链路中传输。

1. 电子商务

本知识点主要在于让考生掌握电子商务安全的基本需求、安全协议以及相关的技术。

(1) 电子商务安全特性

电子商务是指利用简单、快捷、低成本的电子通信方式, 买卖双方不谋面地进行各种商贸活动。对电子商务安全需求主要表现在以下几个方面。

- ① 有效性：要对网络故障、操作错误、应用程序错误、硬件故障、系统软件错误及计算机病毒所产生的潜在威胁加以控制和预防，以保证贸易数据在确定的时刻、地点是有效的。
- ② 机密性：要预防非法的信息存取和信息在传输过程中被非法窃取。
- ③ 数据完整性：要求能够保证数据的一致性，防止数据被非授权者建立、修改和破坏。
- ④ 不可抵赖性：也就是防止交易的某一方否认曾经发生的交易行为。
- ⑤ 审查能力：根据机密性和完整性的要求，应对数据审查的结果进行记录。

与电子商务相关的安全技术主要包括：VPN、SSL、电子邮件安全协议（包括 PEM、S/MIME、MOSS）、电子支付安全性等。

（2）SSL/SET 和 SHTTP

SSL（安全套接层）是工作在传输层的安全协议。它结合了信息加/解密、数字签名与鉴证两大技术。它包括协商层（SSL Handshake）和记录层（SSL Record）两个部分。

① 协商层：包括“沟通”通信中所使用的 SSL 版本、信息加密用的算法、所使用的公钥算法，并要求用公钥方式对客户端进行身份认证。

② 记录层：对应用程序提供的信息进行分段、压缩、数据认证与加密，能够保障数据的机密性和报文的完整性。整个操作步骤如下。

- a. 分片，分成 214 字节或更小的数据块。
- b. 可选地应用压缩。
- c. 使用共享的密钥计算出报文鉴别代码。
- d. 使用同步算法加密。
- e. 附加首部，包括内容类型、主要版本、次要版本、压缩长度。

SHTTP 是在 HTTP 协议上的扩展，目的是保证商业贸易的传输安全，工作于应用层。由于 SSL 的迅速出现，加上 SSL 工作在传输层，适用于所有 TCP/IP 应用；而 SHTTP 只能够工作于 HTTP 协议层，只限于 Web 应用，因此 SHTTP 并未能够获得广泛应用。

SET 协议是 Visa 与 MasterCard 共同制定的一套安全又方便的交易模式，最早用于支持各种信用卡的交易。SSL 在使用时，只要求服务器端拥有数字证书，而 SET 则同时要求客户端需要数字证书。SET 可以实现：为交易涉及的各方之间提供安全的通信信道，通过使用 X.509 数字证书来提供信任，可以保证信息的机密性。

SET 协议的参与者有：卡用户（网上交易发起方）、商人（网上交易服务商）、发行人——银行（信用卡持卡人）、获得者（处理交易的金融机构）、支付网关和 CA 中心（发放证书者）。

（3）PGP 技术

PGP 协议在互联网上广泛被采用，特别在 E-mail 的保护上应用更广，它是结合了 RSA 和 IDEA 的链式加密法。PGP 的工作过程是用一个随机生成的密钥（每次加密不同）使用 IDEA 算法对明文加密，然后用 RSA 算法对该密钥加密。因此它既有了 RSA 的保密性，又获得了 IDEA 算法的快捷性。

（4）Kerberos

在分布式网络应用环境中，要保证其使用的安全性，就必须让工作站能够用可信、安全的方式向服务器证实其身份，否则就会出现许多安全问题。而解决这个问题的技术称之为身份认证。比较常见的身份认证技术包括：用户双方指定共享密钥（最不安全）、使用智能卡生成密钥、使用 Kerberos 服务、使用 PKI 服务（即通过从 CA 中心获取数字证书的方式）。

Kerberos 并非为每一个服务器构造一个身份认证协议，而是提供一个中心认证服务器，提供用户到服务器以及服务器到用户的认证服务。Kerberos 的核心是使用 DES 加密技术，实现最基本的认证服务。

如图 11-6 所示，Kerberos 认证过程可以分为 3 个阶段，共 6 个步骤。

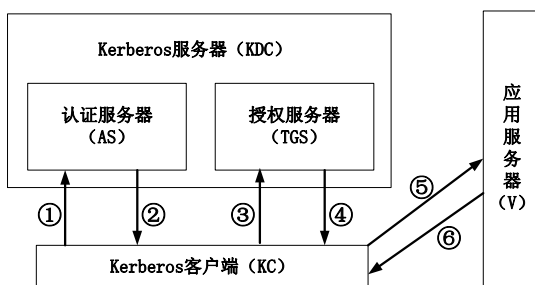


图 11-6 Kerberos 工作原理示意图

第一阶段：认证服务交换，客户端获取授权服务器访问许可票据。

① 用户 A 输入自己的用户名，以明文的方式发给认证服务器。

② 认证服务器返回一个会话密钥 KS 和一个票据 KTGS (A,KS)，这个会话密钥是一次性的（也可以使用智能卡生成），而这两个数据报则是使用用户 A 的密钥加密的，返回时将要求其输入密码，并解密数据。

第二阶段：票据许可服务交换，客户端获得应用服务访问许可票据。

③ 用户 A 将获得的票据、要访问的应用服务器名 B，以及用会话密钥加密的时间标记（用来防止重发攻击）发送给授权服务器（TGS）。

④ 授权服务器（TGS）收到后，返回 A 和 B 通信的会话密钥，包括用 A 的密钥加密的，和 B 的密钥加密的会话密钥 KAB。

第三阶段：客户端与应用服务器认证交换，客户端最终获得应用服务。

⑤ 用户 A 将从 TGS 收到的用 B 的密钥加密的会话密钥发给服务器 B，并且附上用双方的会话密钥 KAB 加密的时间标记以防止重发攻击。

⑥ 服务器 B 进行应答，完成认证过程。

从上面的描述中可以看出，Kerberos 采用了连续加密的机制来防止会话被劫持。

2. 虚拟专用网

本知识点重点在于让考生掌握 VPN 的概念，了解其关键的实现技术，特别是各种隧道技术的特点与实现，了解 4 种 VPN 参考模型，以及 3 种 VPN 分类。

虚拟专用网是企业网在因特网等公共网络上的延伸，通过一个私有的通道在公共网络上创建一个安全的私有连接。因此，从本质上说 VPN 是一个虚信道，它可用来连接两个专用网，通过可靠的加密技术方法保证其安全性，并且是作为一个公共网络的一部分存在的。

图 11-7 所示的就是一个 VPN 构成的原理示意图。

(1) VPN 的关键技术

一个完整的 VPN 技术方案中包括 VPN 隧道技术、密码技术和服务质量保证技术。

隧道技术就是一种数据封装协议，即将一种协议封装在另一种协议中传输，从而实现被封装协议对封装协议的透明性。常见的隧道技术可以根据其工作的层次分为两类：一是“二

层隧道技术”，包括 PPP 基础上的 PPTP（点到点隧道协议）和 L2F（二层转发协议）、L2TP（二层隧道协议）；二是“三层隧道技术”，主要代表是 IPSec（IP 层安全协议，它是 IPv4 和 IPv6 的安全标准）、移动 IP 协议和虚拟隧道协议（VTP）。

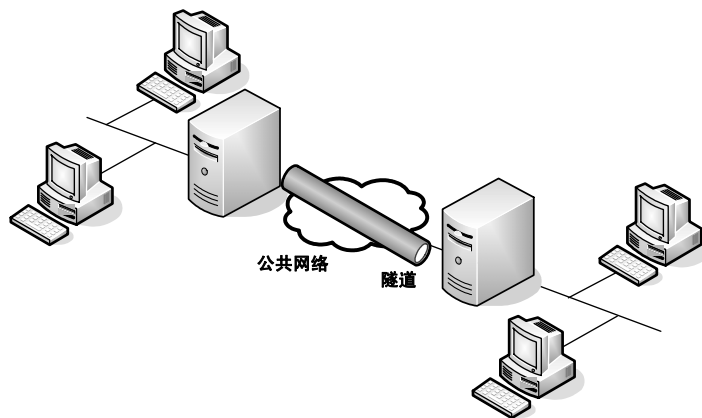


图 11-7 VPN 构成原理示意图

密码技术在 VPN 中采用的密码技术包括加/解密、身份认证、密钥管理等。

QoS 机制包括 RSVP（资源预留协议）和 SBM（子网带宽管理）。

(2) VPN 的分类与应用

VPN 的分类与应用如表 11-7 所示。

表 11-7 VPN 的分类与应用

分 类	特 点	应 用
Intranet VPN	可在 Internet 上组建世界范围的 VPN 网络	企业内部各分支机构互联
Access VPN	通过一个拥有专用网络相同策略的共享基础设施，提供对企业内/外部网的远程访问	企业的内部人员移动或远程办公需要
Extranet VPN	通过使用一个专用连接的共享基础设施，将供应商、合作伙伴连接到企业内部网络	提供 B2B 之间的安全访问服务

(3) VPN 隧道技术

VPN 隧道技术主要包括 PPTP、L2F、L2TP 和 IPSec，其中前三者的比较如表 13-11 所示。

表 11-8 VPN 隧道技术

项 目	PPTP	L2F	L2TP
对底层介质的要求	IP 网络	没有要求	没有要求
消息的构造格式	固化构造	选项构造	属性构造
端对端身份认证	依赖 PPP	全程	全程
隧道和会话维护	有	没有	有
流量控制特性	序列号和确认、滑动窗口	很弱	会话的计数和计时器

① PPTP：在逻辑上延伸了 PPP 会话，从而形成了虚拟的远程拨号。在协议实现时，使用了与 PPP 相同的认证机制，包括 EAP（扩展身份认证协议）、MS-CHAP（微软挑战握手认证协议）、CHAP（挑战握手认证协议）、SPAP（Shiva 口令字认证协议）、PAP（口令字认

证协议)。

② L2F: 可以在多种介质上建立多协议的安全 VPN 通信方式, 它将数据链路层的协议封装起来, 以使网络的数据链路层完全独立于用户的数据链路层协议。

③ L2TP: 是 PPTP 和 L2F 结合的产物。L2TP 协议将 PPP 帧封装后, 可以通过 IP、X.25、FR 或 ATM 进行传输。创建 L2TP 隧道时必须使用与 PPP 连接相同的认证机制, 它结合了 L2F 和 PPTP 的优点, 可以让用户从客户端或接入服务器端发起 VPN 连接。

④ IPSec: 是由安全协议、密钥管理协议、安全关联、认证和加密算法 4 部分构成的安全结构。安全协议在 IP 协议中增加两个基于密码的安全机制——认证头 (AH) 和封装安全载荷 (ESP), 前者支持 IP 数据项的可认证性和完整性, 后者实现了通信的机密性。密钥管理协议 (密钥交换手工和自动 IKE) 定义了通信实体间身份认证、创建安全关联、协商加密算法、共享会话密钥的方法。

(4) PPP 会话过程

PPP 拨号会话过程可以分成 4 个不同的阶段, 分别是: 创建 PPP 链路、用户验证、PPP 回叫控制、调用网络层协议。在第 2 个阶段, 客户 PC 会将用户的身份明发给远端的接入服务器。该阶段使用一种安全认证方式避免第三方窃取数据或冒充远程客户接管与客户端的连接。大多数的 PPP 方案只提供了有限的认证方式, 包括口令字认证协议 (PAP), 挑战握手认证协议 (CHAP) 和微软挑战握手认证协议 (MS-CHAP)。

① 口令字认证协议 (PAP)。PAP 是一种简单的明文认证方式。NAS 要求用户提供用户名和口令, PAP 以明文方式返回用户信息。很明显, 这种认证方式的安全性较差, 第三方可以很容易地获取被传送的用户名和口令, 并利用这些信息与 NAS 建立连接, 获取 NAS 提供的所有资源。所以, 一旦用户密码被第三方窃取, PAP 无法提供避免受到第三方攻击的保障措施。

② 挑战握手认证协议 (CHAP)。CHAP 是一种加密的认证方式, 能够避免建立连接时传送用户的真实密码。NAS 向远程用户发送一个挑战口令 (challenge), 其中包括会话 ID 和一个任意生成的挑战字串。远程客户必须使用 MD5 单向哈希算法返回用户名和加密的挑战口令、会话 ID 以及用户口令, 其中用户名以非哈希方式发送。CHAP 为每一次认证任意生成一个挑战字串来防止受到再现攻击。在整个连接过程中, CHAP 将不时地向客户端重复发送挑战口令, 从而避免第三方冒充远程客户进行攻击。

11.5.2 一点一练

试题 1

支持安全 WEB 服务的协议是____(1)_____。

- (1) A. HTTPS B. WINS C. SOAP D. HTTP

试题 2

安全电子邮件使用____(2)_____协议。

- (2) A. PGP B. HTTPS C. MIME D. DES 次

试题 3

Kerberos 由认证服务器 (AS) 和票证授予服务器 (TGS) 两部分组成, 当用户 A 通过 Kerberos 向服务器 V 请求服务时, 认证过程如图 11-8 所示, 图中①处为____(3)____, ②处为____(4)_____。

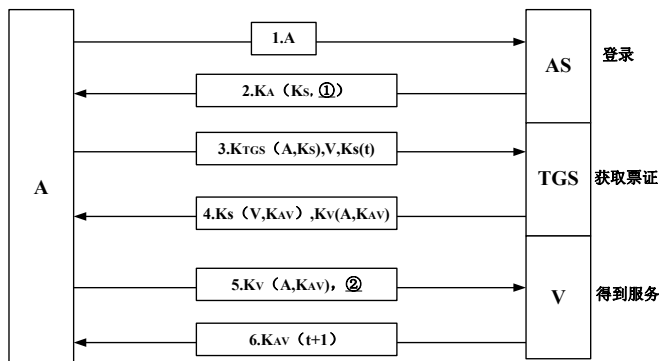


图 11-8 kerberos 工作原理图

- (3) A. $K_{TGS}(A, K_S)$ B. $K_S(V, K_{AV})$ C. $K_V(A, K_{AV})$ D. $K_S(t)$
 (4) A. $A.K_{AV}(t+1)$ B. $K_S(t+1)$ C. $K_S(t)$ D. $K_{AV}(t)$

试题 4

HTTPS 的安全机制工作在__(5)__, 而 S-HTTP 的安全机制工作在__(6)__。

- (5) A. 网络层 B. 传输层 C. 应用层 D. 物理层
 (6) A. 网络层 B. 传输层 C. 应用层 D. 物理层

试题 5

HTTPS 采用__(7)__协议实现安全网站访问。

- (7) A. SSL B. Ipsec C. PGP D. SET

11.5.3 解析与答案

试题 1 分析

HTTPS 是以安全为目标的 HTTP 通道, 简单地讲是 HTTP 的安全版。即 HTTP 下加入 SSL 层, HTTPS 的安全基础是 SSL, 因此加密的详细内容就需要 SSL。

试题 1 答案

- (1) A

试题 2 分析

PGP 是一个基于 RSA 公钥加密体系的邮件加密协议。可以用它对邮件保密以防止非授权者阅读, 它还能对邮件加上数字签名从而使收信人可以确认邮件的发送者, 并能确信邮件没有被篡改。

试题 2 答案

- (2) A

试题 3 分析

Kerberos 并非为每一个服务器构造一个身份认证协议, 而是提供一个中心认证服务器, 提供用户到服务器以及服务器到用户的认证服务。Kerberos 的核心是使用 DES 加密技术, 实现最基本的认证服务。

如图 11-9 所示, Kerberos 认证过程可以分为 3 个阶段, 6 个步骤。

第一阶段: 认证服务交换, 客户端获取授权服务器访问许可票据。

① 用户 A 输入自己的用户名, 以明文的方式发给认证服务器。

② 认证服务器返回一个会话密钥 K_S 和一个票据 $K_{TGS}(A, K_S)$, 这个会话密钥是一次性的 (也可以使用智能卡生成), 而这两个数据报则是使用用户 A 的密钥加密的, 返回时将

要求其输入密码，并解密数据。

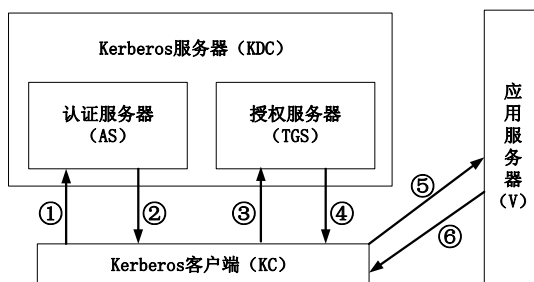


图 11-9 Kerberos 工作原理示意图

第二阶段：票据许可服务交换，客户端获得应用服务访问许可票据。

③ 用户 A 将获得的票据、要访问的应用服务器名 B，以及用会话密钥加密的时间标记（用来防止重发攻击）发送给授权服务器（TGS）。

④ 授权服务器（TGS）收到后，返回 A 和 B 通信的会话密钥，包括用 A 的密钥加密的，和 B 的密钥加密的会话密钥 K_{AB}。

第三阶段：客户端与应用服务器认证交换，客户端最终获得应用服务。

⑤ 用户 A 将从 TGS 收到的用 B 的密钥加密的会话密钥发给服务器 B，并且附上用双方的会话密钥 K_{AB} 加密的时间标记以防止重发攻击。

⑥ 服务器 B 进行应答，完成认证过程。

从上面的描述中可以看出，Kerberos 采用了连续加密的机制来防止会话被劫持。

试题 3 答案

(3) A

(4) D

试题 4 分析

HTTP 是超文本传输协议，信息是明文传输，HTTPS 则是具有安全性的 SSL 加密传输协议。S-HTTP 即安全超文本传输协议。它是一种面向安全信息通信的协议，它可以和 HTTP 结合起来使用。

试题 4 答案

(5) B

(6) C

试题 5 分析

HTTPS 实际上采用了 Netscape 的安全套接字层（SSL）作为 HTTP 应用层的子层。通过端口 443 进行通信。而 SSL 使用的是 40 位关键字作为 RC4 流加密算法。HTTPS 和 SSL 支持使用 X.509 数字认证，因此可以确认发送者的身份。此题中给出的其他选项都不满足条件，如 B 的 IPsec 是一个基于 IP 层的安全协议，用于 VPN。PGP 是一个加密算法，通常用于电子邮件的加密。SET 是基于网上使用信用卡安全支付的一个标准。

试题 5 答案

(7) A

11.6 考前冲刺

试题 1

在 Kerberos 认证系统中，用户首先向____(1)____申请初始票据，然后从____(2)____获得会话密钥。

- (1) A. 域名服务器 DNS B. 认证服务器 AS
C. 票据授予服务器 TGS D. 认证中心 CA
- (2) A. 域名服务器 DNS B. 认证服务器 AS
C. 票据授予服务器 TGS D. 认证中心 CA

试题 2

按照 RSA 算法, 若选两奇数 $p=5$, $q=3$, 公钥 $e=7$, 则私钥 d 为 (3)。

- (3) A. 6 B. 7 C. 8 D. 9

试题 3

报文摘要算法 MD5 的输出是 (4) 位, SHA-1 的输出是 (5) 位。

- (4) A. 56 B. 128 C. 160 D. 168
(5) A. 56 B. 128 C. 160 D. 168

试题 4

公钥体系中, 私钥用于 (6), 公钥用于 (7)。

- (6) A. 解密和签名 B. 加密和签名 C. 解密和认证 D. 加密和认证
(7) A. 解密和签名 B. 加密和签名 C. 解密和认证 D. 加密和认证

试题 5

以下关于加密算法的叙述中, 正确的是 (8)。

- (8) A. DES 算法采用 128 位的密钥进行加密
B. DES 算法采用两个不同的密钥进行加密
C. 三重 DES 算法采用 3 个不同的密钥进行加密
D. 三重 DES 算法采用两个不同的密钥进行加密

试题 6

在 Kerberos 系统中, 使用一次性密钥和 (9) 来防止重放攻击。

- (9) A. 时间戳 B. 数字签名 C. 序列号 D. 数字证书

试题 7

某网站向 CA 申请了数字证书, 用户通过 (10) 来验证网站的真伪。在用户与网站进行安全通信时, 用户可以通过 (11) 进行加密和验证, 该网站通过 (12) 进行解密和签名。

- (10) A. CA 的签名 B. 证书中的公钥 C. 网站的私钥 D. 用户的公钥
(11) A. CA 的签名 B. 证书中的公钥 C. 网站的私钥 D. 用户的公钥
(12) A. CA 的签名 B. 证书中的公钥 C. 网站的私钥 D. 用户的公钥

试题 8

IPSec 的加密和认证过程中所使用的密钥由 (13) 机制来生成和分发。

- (13) A. ESP B. IKE C. TGS D. AH

试题 9

SSL 协议使用的默认端口是 (14)。

- (14) A. 80 B. 445 C. 8080 D. 443

试题 10

Alice 向 Bob 发送数字签名的消息 M, 则不正确的说法是 (15)。

- (15) A. Alice 可以保证 Bob 收到消息 M
B. Alice 不能否认发送过消息 M

- C. Bob 不能编造或改变消息 M
- D. Bob 可以验证消息 M 确实来源于 Alice

试题 11

在 X.509 标准中, 不包含在数字证书中的数据域是____(16)____。

- (16) A. 序列号 B. 签名算法 C. 认证机构的签名 D. 私钥

试题 12

有两个公司希望通过 Internet 传输大量敏感数据, 从信息源到目的地之间的传输数据以密文形式出现, 而且不希望由于在传输节点使用特殊的安全单元而增加开支, 最合适的加密方式是____(17)____, 使用会话密钥算法效率最高的是____(18)____。

- (17) A. 链路加密 B. 节点加密 C. 端-端加密 D. 混合加密
(18) A. RSA B. RC-5 C. MD5 D. ECC

试题 13

下面关于 ARP 木马的描述中, 错误的是____(19)____。

- (19) A. ARP 木马利用 ARP 协议漏洞实施破坏
B. ARP 木马发作时可导致网络不稳定甚至瘫痪
C. ARP 木马破坏网络的物理连接
D. ARP 木马把虚假的网关 MAC 地址发送给受害主机

试题 14

为了防止电子邮件中的恶意代码, 应该用____(20)____方式阅读电子邮件。

- (20) A. 纯文本 B. 网页 C. 程序 D. 会话

试题 15

常用对称加密算法不包括____(21)____。

- (21) A. DES B. RC-5 C. IDEA D. RSA

试题 16

数字签名功能不包括____(22)____。

- (22) A. 防止发送方的抵赖行为 B. 发送方身份确认
C. 接收方身份确认 D. 保证数据的完整性

试题 17

“TCP SYN Flooding” 建立大量处于半连接状态的 TCP 连接, 其攻击目标是网络的____(23)____。

- (23) A. 保密性 B. 完整性 C. 真实性 D. 可用性

试题 18

TCP/IP 在多个层次引入了安全机制, 其中 TLS 协议位于____(24)____。

- (24) A. 数据链路层 B. 网络层 C. 传输层 D. 应用层

试题 19

计算机感染特洛伊木马后的典型现象是____(25)____。

- (25) A. 程序异常退出 B. 有未知程序试图建立网络连接
C. 邮箱被垃圾邮件填满 D. Windows 系统黑屏

试题 20

在下列安全协议中, ____ (26) ____ 能保证交易双方无法抵赖。

(26) A. SET B. HTTPS C. PGP D. MOSS

试题 21

某银行为用户提供网上服务,允许用户通过浏览器管理自己的银行账户信息。为保障通信的安全,该 Web 服务器可选的协议是____(27)____。

(27) A. POP B. SNMP C. HTTP D. HTTPS

试题 22

安全电子邮件协议 PGP 不支持____(28)____。

(28) A. 确认发送者的身份 B. 确认电子邮件未被修改
C. 防止非授权者阅读电子邮件 D. 压缩电子邮件大小

试题 23

Needham-Schroeder 协议是基于____(29)____的认证协议。

(29) A. 共享密钥 B. 公钥 C. 报文摘要 D. 数字证书

试题 24

实现 VPN 的关键技术主要有隧道技术、加/解密技术、____(30)____和身份认证技术。

(30) A. 入侵检测技术 B. 病毒防治技术 C. 安全审计技术 D. 密钥管理技术

试题 25

如果需要在传输层实现 VPN,可选的协议是____(31)____。

(31) A. L2TP B. PPTP C. TLS D. IPsec

试题 26

某 Web 网站向 CA 申请了数字证书。用户登录该网站时,通过验证____(32)____,可确认该数字证书的有效性。

(32) A. CA 的签名 B. 网站的签名 C. 会话密钥 D. DES 密码

试题 27

DES 是一种____(33)____算法。

(33) A. 共享密钥 B. 公开密钥 C. 报文摘要 D. 访问控制

试题 28

下列行为不属于网络攻击的是____(34)____。

(34) A. 连续不停 Ping 某台主机 B. 发送带病毒和木马的电子邮件
C. 向多个邮箱群发一封电子邮件 D. 暴力破解服务器密码

试题 29

采用 Kerberos 系统进行认证时,可以在报文中加入____(35)____来防止重放攻击。

(35) A. 会话密钥 B. 时间戳 C. 用户 ID D. 私有密钥

试题 30

目前在网络上流行的“熊猫烧香”病毒属于____(36)____类型的病毒。

(36) A. 目录 B. 引导区 C. 蠕虫 D. DoS

11.7 习题解析

试题 1 分析

在 Kerberos 认证系统中,用户首先向认证服务器 AS 申请初始票据,然后从票据授予服务器 TGS 获得会话密钥。

试题 1 答案

(1) B

(2) C

试题 2 分析

本题考查 RSA 的算法知识。

RSA 是一种公钥加密算法，它按照下面的要求选择公钥和密钥：

① 选择两个大素数 p 和 q （大于 10^{100} ）；

② 令 $n=p \times q$ 和 $z=(p-1) \times (q-1)$ ；

③ 选择 d 与 z 互质；

④ 选择 e ，使 $e \times d = 1 \pmod{z}$ 。

从题中举例数据 $p=5$ 、 $q=3$ 、 $e=7$ 可得：

$$n=5 \times 3=15;$$

$$z=(5-1) \times (3-1)=8;$$

$$7 \times d = 1 \pmod{8}.$$

将题中 4 个选项代入上式可知，只有 $d=7$ 满足要求。

试题 2 答案

(3) B

试题 3 分析

本题考查网络安全中报文摘要算法相关知识。

MD5 以 512 位分组来处理输入的信息，且每一分组又被划分为 16 个 32 位子分组，经过了一系列的处理后，算法的输出由 4 个 32 位分组组成，将这 4 个 32 位分组级联后将生成一个 128 位散列值。

SHA（安全散列算法）是由美国国家安全局设计，美国国家标准与技术研究院（NIST）发布的一系列密码散列函数。其中 SHA-1 会从一个最大 2^{64} 位元的信息中产生一串 160 位元的摘要。

试题 3 答案

(4) B

(5) C

试题 4 分析

本题考查公钥体系的理解和应用。

1976 年斯坦福大学的 Diffie 和 Hellman 提出了使用不同的密钥进行加密和解密的公钥加密算法。设 P 为明文， C 为密文， E 为公钥控制的加密算法， D 为私钥控制的解密算法，这些参数满足下列 3 个条件：

① $D(E(P))=P$ ；

② 不能由 E 导出 D ；

③ 选择明文攻击（选择任意明文-密文对以确定未知的密钥）不能破解 E 。

加密时计算 $C=E(P)$ ，解密时计算 $P=D(C)$ 。加密和解密是互逆的。用公钥加密，私钥解密，可实现保密通信；用私钥加密，公钥解密，可实现数字签名。

试题 4 答案

(6) A

(7) D

试题 5 分析

DES 算法是典型的对称加密算法，其密钥长度是 64bit，其中包含校验位 8bit，实际有效长度是 56bit。三重 DES 算法是为了解决 DES 算法的安全问题而提出的，加密过程中使用

了 3 次 DES 算法。分别是用 K1 加密得到密文，用 K2 解密密文，得到新的密文（因为 K2 不等于 K1，所以无法解出明文），再用 K3 加密得到用于发送的密文，通常为了简便，取 $K1=K3$ ，因此实际上只用了两个不同的密钥。长度为 128bit，去掉校验的有效密钥长度是 112bit。

试题 5 答案

(8) D

试题 6 分析

本题考查 Kerberos 系统安全相关知识。

一次性密钥、序列号和时间戳都是对付重放攻击的有效手段，Kerberos 系统采用一次性密钥和时间戳来防止重放攻击。

试题 6 答案

(9) A

试题 7 分析

考查数字证书相关知识。

数字证书是由权威机构——CA 证书授权（Certificate Authority）中心发行的，能提供在 Internet 上进行身份验证的一种权威性电子文档，人们可以在 Internet 交往中用它证明自己的身份和识别对方的身份。

数字证书包含版本、序列号、签名算法标识符、签发人姓名、有效期、主体名和主体公钥信息等并附有 CA 的签名，用户获取网站的数字证书后通过验证 CA 的签名来确认数字证书的有效性，从而验证网站的真伪。

在用户与网站进行安全通信时，用户发送数据时使用网站的公钥（从数字证书中获得）加密，收到数据时使用网站的公钥验证网站的数字签名；网站利用自身的私钥对发送的消息签名和对收到的消息解密。

试题 7 答案

(10) A

(11) B

(12) C

试题 8 分析

本题考查 IPSec 相关知识。

IPSec 密钥管理利用 IKE（Internet 密钥交换协议）机制实现，IKE 解决了在不安全的网络环境（如 Internet）中安全地建立或更新共享密钥的问题。

试题 8 答案

(13) B

试题 9 分析

本题属于记忆题。80 端口是 Web 服务默认端口。8080 端口一般用于局域网内部提供 Web 服务。445 端口和 139 端口一样，用于局域网中共享文件夹或共享打印机。

试题 9 答案

(14) D

试题 10 分析

本题考查数字签名的相关概念。

数字签名设计为发送者不可否认，接收者可以验证但不能编造或篡改。所以选项 B、C 和 D 都是正确的。选项 A 显然是错误的。

试题 10 答案

(15) A

试题 11 分析

本题考查数字证书的基础知识。

数字证书中包含用户的公钥，而用户的私钥只能被用户拥有。所以选项 D 是不可能包含在数字证书中的。

试题 11 答案

(16) D

试题 12 分析

通过 Internet 传输数据，报文在路由器间依据路由选择算法进行转发，所经过的路径并不唯一，故采用链路加密难以实现；节点加密开支过大；混合加密结合多种方式，也不符合题意；端-端加密在发送端与接收端之间进行加/解密，是最合适的加密方式。在传输过程中采用对称密钥比非对称密钥效率要高，故选择 RC-5。

试题 12 答案

(17) C

(18) B

试题 13 分析

本题考查计算机病毒的相关知识。

ARP 木马的工作原理是利用 ARP 协议漏洞，把虚假的网关 MAC 地址发送给受害主机，造成局域网内出现大量的 ARP 消息从而造成网络堵塞。但并没有破坏网络的物理连通性。所以选项 C 是错误的。

试题 13 答案

(19) C

试题 14 分析

本题考查的是电子邮件中恶意代码的相关知识，当电子邮件中包含网页或者程序时，就有可能包含恶意代码。因此，选择以纯文本的方式阅读电子邮件可以防止恶意代码的触发。

试题 14 答案

(20) A

试题 15 分析

本题考查常用加密算法的基本概念。常用加密算法根据加密/解密原理分为对称密钥体制和非对称密钥体制。对称密钥体制加密/解密采用同一个密钥。非对称密钥体制采用私钥加密，公钥解密。DES、RC-5、IDEA 均属于对称密钥体制，RSA 属于非对称密钥体制。所以答案为 D。

试题 15 答案

(21) D

试题 16 分析

本题考查数字签名的概念。数字签名 (Digital Signature) 技术是不对称加密算法的典型应用：数据源发送方使用自己的私钥对数据校验或其他与数据内容有关的变量进行加密处理，完成对数据的合法“签名”，数据接收方则利用对方的公钥来解读收到的“数字签名”，并将解读结果用于对数据完整性的检验，以确认签名的合法性。数字签名主要的功能是：保证信

息传输的完整性、发送者的身份认证、防止交易中的抵赖发生。

数字签名无法实现接收方身份确认，所以答案为 C。

试题 16 答案

(22) C

试题 17 分析

本题考查网络攻击手段和目标。“TCP SYN Flooding”利用 TCP 实现的安全漏洞，建立大量处于半连接状态的 TCP 连接，使得被攻击方消耗大量的资源，从而影响被攻击方的可用性。所以答案为 D。

试题 17 答案

(23) D

试题 18 分析

本题考查 TLS 安全协议的基本概念。TLS (Transport Layer Security Protocol, 传输层安全协议) 用于在两个通信应用程序之间提供保密性和数据完整性，通常位于某个可靠的传输协议 (例如 TCP) 上面，与具体的应用无关。所以，一般把 TLS 协议归为传输层安全协议。答案为 C。

试题 18 答案

(24) C

试题 19 分析

完整的木马程序一般由两个部分组成：一个是服务器程序，一个是控制器程序。计算机感染特洛伊木马后，特洛伊木马的服务器程序会自动运行，并在特定端口上监听，接收控制器端程序的指令，通过运行实时网络连接监控程序可以发现异常连接，据此可以初步判断机器是否被特洛伊木马入侵。所以答案是 B。

试题 19 答案

(25) B

试题 20 分析

本题考查 SET 协议的基本概念。SET (Secure Electronic Transaction, 安全电子交易) 协议的主要目的是保证用户、商家和银行之间通过信用卡支付的交易过程中支付信息的保密、支付过程的完整、商户及持卡人的合法身份确认。

HTTPS 是安全 HTTP 协议，PGP 和 MOSS 都是安全电子邮件协议。

试题 20 答案

(26) A

试题 21 分析

POP 是邮局协议，用于接收邮件；SNMP 是简单网络管理协议，用于网络管理；HTTP 是超文本传输协议，众多 Web 服务器都使用 HTTP，但是它不是安全的协议；HTTPS 是安全的超文本传输协议。

试题 21 答案

(27) D

试题 22 分析

本题考查安全电子邮件协议 PGP 的基本知识。安全电子邮件协议 PGP

(Pretty Good Privacy) 在电子邮件安全实施中被广泛采用, PGP 通过单向散列算法对邮件内容进行签名, 以保证信件内容无法被修改, 使用公钥和私钥技术保证邮件内容保密且不可否认。发信人与收信人的公钥都保存在公开的地方, 公钥的权威性则可以由第三方进行签名认证。在 PGP 系统中, 信任是双方的直接关系。

试题 22 答案

(28) D

试题 23 分析

本题考查有关 Needham-Schroeder 协议的基础知识。考生应该知道 Needham-Schroeder 协议是基于共享密钥进行认证的协议。

试题 23 答案

(29) A

试题 24 分析

本题考查 VPN 方面的基础知识。考生应该知道实现 VPN 的关键技术主要有隧道技术、加/解密技术、密钥管理技术和身份认证技术。

试题 24 答案

(30) D

试题 25 分析

L2TP、PPTP 是两种链路层的 VPN 协议, TLS 是传输层 VPN 协议, IPsec 是网络层 VPN 协议。

试题 25 答案

(31) C

试题 26 分析

本题考查公钥基础设施方面有关数字签名的基础知识。数字证书能够验证一个实体身份, 而这是在保证数字证书本身有效性这一前提下才能够实现的。验证数字证书的有效性是通过验证颁发证书的 CA 的签名实现的。

试题 26 答案

(32) A

试题 27 分析

DES (Data Encryption Standard) 是美国政府于 1977 年采用的加密标准, 最初是由 IBM 公司在 20 世纪 70 年代初期开发的。美国政府在 1981 年又将 DES 进一步规定为 ANSI 标准。

DES 是一个对称密钥系统, 加密和解密使用相同的密钥。它通常选取一个 64 位 (bit) 的数据块, 使用 56 位的密钥, 在内部实现多次替换和变位操作来达到加密的目的。

试题 27 答案

(33) A

试题 28 分析

网络攻击是以网络为手段窃取网络上其他计算机的资源或特权, 对其安全性或可用性进行破坏的行为。网络攻击又分为主动攻击和被动攻击。被动攻击就是网络窃听, 截取数据包并进行分析, 从中窃取重要的敏感信息。被动攻击很难被发现, 因此预防很重要, 防止被动攻击的主要手段是数据加密传输。为了保护网络资源免受威胁和攻击, 在密码学及安全协议

的基础上发展了网络安全体系中的 5 类安全服务，它们是：身份认证、访问控制、数据保密、数据完整性和不可否认。对这 5 类安全服务，国际标准化组织 ISO 已经有了明确的定义。主动攻击包括窃取、篡改、假冒和破坏。字典式口令猜测，IP 地址欺骗和服务拒绝攻击等都属于主动攻击。一个好的身份认证系统（包括数据加密、数据完整性校验、数字签名和访问控制等安全机制）可以用于防范主动攻击，但要想杜绝主动攻击很困难，因此对付主动攻击的另一措施是及时发现并及时恢复所造成的破坏，现在有很多实用的攻击检测工具。

常用的有以下 9 种网络攻击方法：获取口令、放置特洛伊木马程序、WWW 的欺骗技术、电子邮件攻击、通过一个节点来攻击其他节点、网络监听、寻找系统漏洞、利用账号进行攻击、偷取特权。

试题 28 答案

(34) C

试题 29 分析

Kerberos 认证是一种使用对称密钥加密算法来实现通过可信第三方密钥分发中心的身份认证系统。客户方需要向服务器方递交自己的凭据来证明自己的身份，该凭据是由 KDC 专门为客户方和服务器方在某一阶段内通信而生成的。凭据中包括客户方和服务器方的身份信息和在下一阶段双方使用的临时加密密钥，还有证明客户方拥有会话密钥的身份认证者信息。身份认证信息的作用是防止攻击者在将来将同样的凭据再次使用。时间标记是检测重放攻击。

试题 29 答案

(35) B

试题 30 分析

熊猫烧香是一种感染型的蠕虫病毒，它能感染系统中.exe、.com、.pif、.src、.html 和.asp 等文件，还能中止大量的反病毒软件进程并且会删除扩展名为.gho 的文件，该文件是系统备份工具 GHOST 的备份文件，使用户的系统备份文件丢失。

被感染的用户系统中所有.exe 可执行文件图标全部被改成熊猫举着三根香的模样。

试题 30 答案

(36) C

网络应用服务器配置

网络应用服务器运维技能是网络工程人员必备的职业技能。在工作中主要体现在网络服务器选型和搭建,应用服务器的运维和优化,根据服务器的及时数据和报表数据执行相应网络管理行为等活动上。

12.1 考点脉络

本章是网络工程师考试的一个必考点,其分值主要集中在下午题部分。根据考试大纲,要求考生掌握以下几个方面的内容。

(1) Web 服务器:主要考查 Windows 下 IIS 组件中 Web 服务器、Linux 下 Apache 服务器配置。

(2) FTP 服务器:主要考查 Windows 下 IIS 组件中 FTP 服务器。

(3) DNS 服务器:主要考查 Windows 和 Linux 系统下 DNS 服务器的配置。

(4) DHCP:主要考查 Windows 和 Linux 系统下 DHCP 服务器的配置。

(5) 文件共享打印服务器:主要考查 Linux 系统下 Samba 服务器的配置。

(6) 代理服务器:主要考查代理服务器的工作原理。

从历年的考试试题来看,本章的考点在综合知识考试中的平均分数为 5 分,约为总分的 7%。而在下午考试中,本章知识占有较大的比重,最多时为 30 分,最少也有 15 分。

考试试题分数主要集中在 Windows 系统下 DNS 服务器、DHCP 服务器、Web 服务器、FTP 服务器、代理服务器等的配置, Linux 系统下 Samba 共享服务器、DHCP 服务器、DNS 服务器、Apache 服务器这 9 个知识点上。

12.2 IIS 组件子服务配置

在 Windows 下 IIS 组件子服务配置这个考点中,主要涉及两个方面的知识,分别是 Windows 系统 IIS 组件下 Web 服务器配置、Windows 系统 IIS 组件下 FTP 服务器配置。

在 Windows Server 2003 中,安装 IIS 有三种途径:利用“管理您的服务器”向导,利用控制面板“添加或删除程序”的“添加/删除 Windows 组件”功能,或者执行无人值守安装。

12.2.1 考点精讲

Windows 系统 IIS 组件下 Web 服务器配置是基于 Windows Server 2003 系统搭建的网站服务器。

Windows 系统 IIS 组件下 FTP 服务器配置是基于 Windows Server 2003 系统搭建的文件传输服务器,以提供企业文件、资料的上传和下载。

1. Web 服务器配置

下面主要介绍 IIS 的设置。

(1) 站点主目录

安装 IIS 后，系统会自动创建一个默认 Web 站点和一个默认 FTP 站点供用户使用。其中，Web 站点与 FTP 站点的默认主目录分别是：“%SYSTEMROOT%\Inetpub\wwwroot”和“%SYSTEMROOT%\Inetpub\ftproot”，其中 SYSTEMROOT 是操作系统根目录。

主目录确定后，用户只需要将要发布的内容复制到该目录下即可。主目录的设置步骤如下。

① 选择“开始”→“程序”→“管理工具”→“Internet 服务管理器”命令，打开“Internet 信息服务”管理器窗口，如图 12-1 所示。

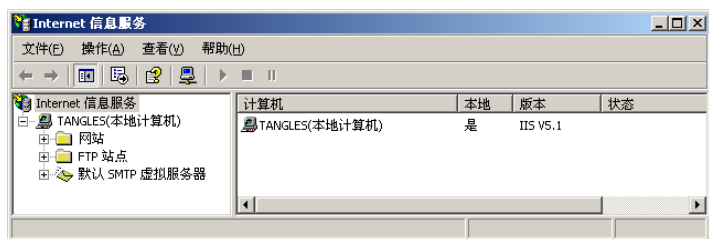


图 12-1 “Internet 信息服务”管理器窗口

② 在控制台目录树中，展开服务器节点，右击“网站”节点，从弹出的快捷菜单中选择“属性”命令，打开“默认网站属性”对话框，并切换到“主目录”选项卡，如图 12-2 所示。

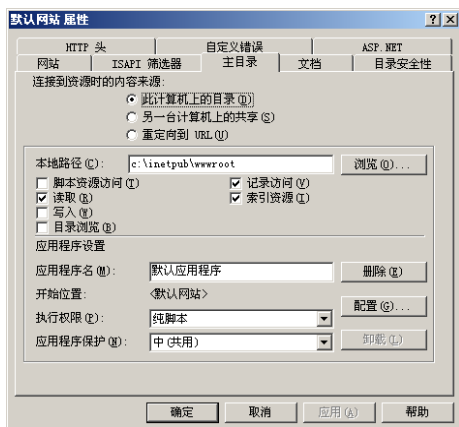


图 12-2 设置主目录

③ 选择“此计算机上的目录”单选框，并在“本地路径”中输入主目录在本地计算机上的路径。通过启用或禁用复选框，来设置主目录的访问权限，如勾选“索引资源”复选框。

目录路径、访问权限及应用程序设置好之后，确定完成主目录的设置。

(2) 站点虚拟目录

要从主目录以外的其他目录中进行内容发布，就必须创建虚拟目录。“虚拟目录”不包含在主目录中，但显示给客户浏览器时却像位于主目录中一样。虚拟目录和实际目录都显示在 Internet 信息服务管理器中。虚拟目录由右下角带有地球的文件夹的图标来表示。对于简单的 Web 站点，不需要添加虚拟目录，而将所有文件放置在站点的主目录中。但是，如果

站点比较复杂, 或者需要为站点的不同部分指定不同的 URL 时, 就需要创建虚拟目录。

创建虚拟目录的操作步骤如下。

① 打开“Internet 信息服务”管理器窗口, 在控制台目录树中展开服务器节点。

② 右击“网站”节点, 从弹出的快捷菜单中选择“新建”→“虚拟目录”命令, 打开“虚拟目录创建向导”对话框。单击“下一步”按钮, 打开“虚拟目录创建向导”对话框的“虚拟目录别名”界面, 如图 12-3 所示。

③ 在图 12-3 中, 在“别名”文本框中输入用于获得此 Web 虚拟目录访问权限的别名。单击“下一步”按钮, 打开“网站内容目录”界面, 如图 12-4 所示, 输入虚拟目录的路径。

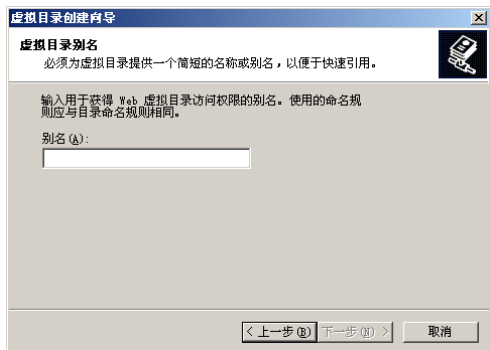


图 12-3 “虚拟目录别名”对话框

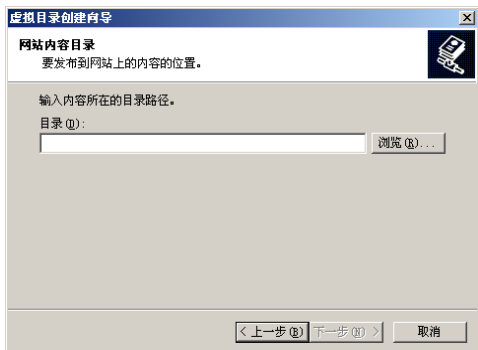


图 12-4 设置 Web 站点内容目录

④ 在图 12-4 中, 单击“下一步”按钮, 打开“访问权限”界面。在“允许下列权限”选项组中, 为此目录设置访问权限, 如图 12-5 所示。

⑤ 在图 12-5 中, 单击“下一步”按钮, 打开“您已成功完成‘虚拟目录创建向导’”界面, 完成虚拟目录的创建。

(3) 默认文档

默认文档是指在浏览器请求指定文档名时提供的文档, 它可以是目录的主页, 也可以是包含站点文档目录列表的索引页。启用默认文档的操作步骤如下。

① 打开“Internet 信息服务”管理器窗口, 在控制台目录树中, 右击要添加页脚文件的 Web 站点或目录, 从弹出的快捷菜单中选择“属性”命令, 打开“默认网站属性”对话框, 并切换到“文档”选项卡, 如图 12-6 所示。

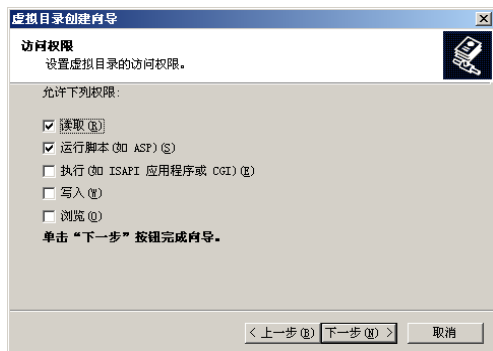


图 12-5 设置访问权限

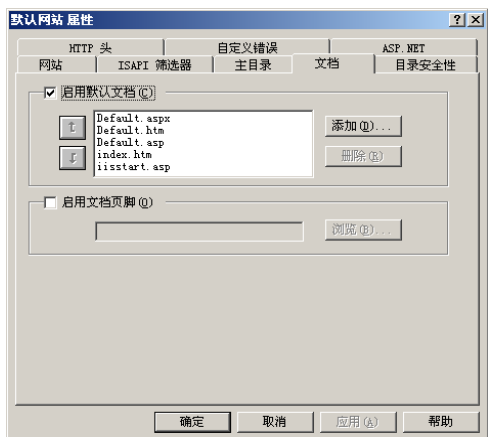


图 12-6 “文档”选项卡

② 在图 12-6 中, 选择“启用默认文档”复选框, 则系统默认文档为 Default.htm 和 Default.asp。如果管理员要添加默认文档, 可单击“添加”按钮, 打开“添加默认文档”对话框, 输入文档名, 确定后, 系统将会按出现在列表中文档名称的顺序提供默认文档, 并返回所找到的第一个文档。

如果要更改搜索顺序, 可选择一个文档, 然后单击箭头按钮; 要从列表中删除默认文档, 可单击“删除”按钮。

2. FTP 服务器配置

FTP 是一种 C/S 结构, 用户启动 FTP 客户机程序, 通过输入用户名和口令, 试图与 FTP 服务器建立连接。一旦成功, 客户机和服务器之间就建立起一条命令链路(控制链路, 交换端口为 21), 其结构如图 12-7 所示。如果用户做好了下载文件的准备, FTP 服务器将开辟一条数据链路(交换端口为 20), 进行所需文件(二进制文件或文本文件)的传送。文件传送结束后, 数据链路被关闭。同时, FTP 服务器通过控制链路发送一个文件结束确认信息。

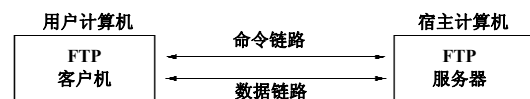


图 12-7 C/S 结构的 FTP

与 Web 站点一样, 每个 FTP 站点也必须有一个主目录, 作为其他访问者访问用户 FTP 站点的起点。在 FTP 站点中, 所有的文件都存放在作为根目录的主目录中, 这就使其他访问者对用户 FTP 站点中的文件查找变得非常方便。设置主目录与虚拟目录的操作步骤参照 Web 服务器的配置。

(1) 创建 FTP 站点

创建 FTP 站点的操作步骤如下。

① 打开“Internet 信息服务”管理器窗口, 展开服务器节点。右击“默认 FTP 站点”, 从弹出的快捷菜单中选择“新建”→“站点”命令, 打开“网站创建向导”对话框中的“FTP 站点创建向导”界面。

② 单击“下一步”按钮, 打开“IP 地址和端口设置”界面, 如图 12-8 所示。在“IP 地址”下拉列表框中选择或直接输入 IP 地址; 在“TCP 端口”文本框中输入 TCP 端口值, 默认值为 21。

③ 在图 12-8 中, 单击“下一步”按钮, 打开“FTP 站点内容目录”界面, 如图 12-9 所示。在“路径”文本框中输入主目录的路径, 或单击“浏览”按钮, 选择路径。

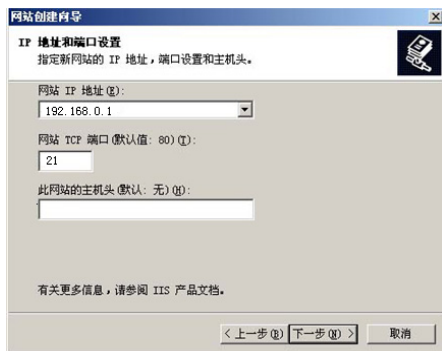


图 12-8 设置 IP 地址和端口

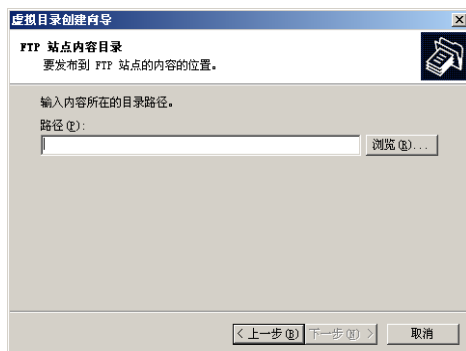


图 12-9 输入站点主目录的路径

④ 在图 12-9 中,单击“下一步”按钮,打开 FTP 站点“访问权限”界面,如图 12-10 所示。在“允许下列权限”选项组中,设置主目录的访问权限。

⑤ 在图 12-10 中,单击“下一步”按钮,打开“您已成功完成‘FTP 站点创建向导’”界面,然后单击“完成”按钮,完成站点的创建。

(2) 设置虚拟目录权限

在 FTP 的虚拟根目录中,必须设置写权限才能发布信息。为了提高安全性,可以在准备向服务器发布信息时设置该权限,并在发布结束后立即消除权限。为 FTP 的虚拟目录设置写权限的操作步骤如下。

① 打开“Internet 信息服务”管理器窗口,展开服务器节点。

② 在“默认 FTP 站点”中,右击“属性”节点,从弹出的快捷菜单中选择“默认 FTP 站点属性”命令,打开“默认 FTP 站点属性”对话框,如图 12-11 所示。

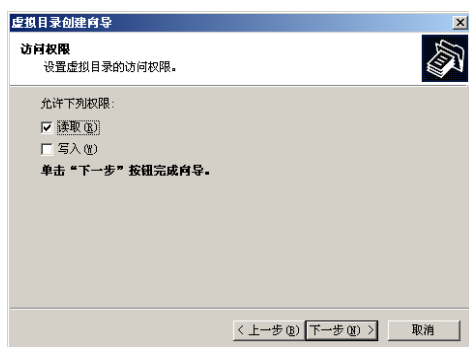


图 12-10 设置主目录的访问权限

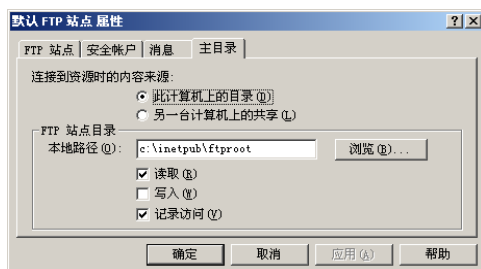


图 12-11 “默认 FTP 站点属性”对话框

③ 在图 12-11 中,在“主目录”选项卡的“FTP 站点目录”选项组中,选择“写入”复选框,添加写权限。最后单击“确定”按钮,保存设置。

(3) 为已知 FTP 用户建立账户

如果用户未被授权访问某台 Internet 主机,则无法在该主机登录,因此,为了保证 FTP 用户能够顺利登录,应为他们建立账户。为已知 FTP 用户建立账户的操作步骤如下。

① 打开“Internet 信息服务”管理器窗口,并展开服务器节点。右击“默认 FTP 站点”节点,从弹出的快捷菜单中选择“属性”命令,打开“默认 FTP 站点属性”对话框。切换到“安全帐户”选项卡,如图 12-12 所示。

② 在图 12-12 中,取消勾选“只允许匿名连接”复选框,此时将弹出一个消息对话框,表明可能通过网络传输未加密的密码,单击“是”按钮即可。在“FTP 站点操作员”选项组中单击“添加”按钮,打开“选择用户”对话框,如图 12-13 所示。

③ 在图 12-13 中,在“名称”列表选择一个或多个用户名,然后单击“确定”按钮。

(4) 常见 FTP 客户端操作命令

- FTP>!: 从 FTP 子系统退出到外壳。
- FTP>?: 显示 FTP 命令说明。? 与 help 相同。

格式: ?[command]。

说明: [command]指定需要帮助的命令名称。如果没有指定 command,FTP 将显示全部命令的列表。

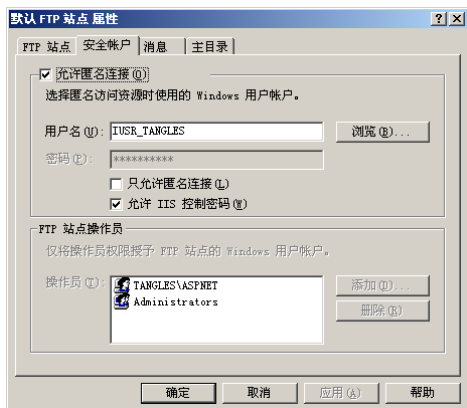


图 12-12 “安全帐户”选项卡

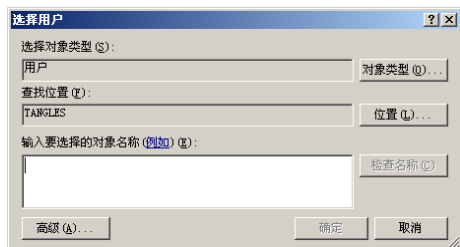


图 12-13 “选择用户”对话框

- FTP> cd: 更改远程计算机上的工作目录。

格式: cd remote-directory。

说明: remote-directory 指定要更改的远程计算机上的目录。

- FTP> delete: 删除远程计算机上的文件。

格式: delete remote-file。

说明: remote-file 指定要删除的文件。

- FTP> dir: 显示远程目录文件和子目录列表。

格式: dir [remote-directory] [local-file]。

说明: remote-directory 指定要查看其列表的目录。如果没有指定目录, 将使用远程计算机中的当前工作目录。local-file 指定要存储列表的本地文件。如果没有指定, 输出将显示在屏幕上。

- FTP> get: 使用当前文件转换类型将远程文件复制到本地计算机。

格式: get remote-file [local-file]。

说明: remote-file 指定要复制的远程文件。local-file 指定要在本地计算机上使用的名称。如果没有指定, 文件将命名为 remote-file。

- FTP> put: 使用当前文件传送类型将本地文件复制到远程计算机上。

格式: put local-file [remote-file]。

说明: local-file 指定要复制的本地文件。remote-file 指定要在远程计算机上使用的名称。如果没有指定, 文件将命名为 local-file。

- FTP> pwd: 显示远程计算机上的当前目录。

- FTP> quit: 结束与远程计算机的 FTP 会话并退出 FTP。

12.2.2 一点一练

试题 1

IIS 6.0 支持的身份验证安全机制有 4 种验证方法, 其中安全级别最高的验证方法是 (1)。

- (1) A. 匿名身份验证
C. 基本身份验证

- B. 集成 Windows 身份验证
D. 摘要式身份验证

试题 2

如图 12-14 所示为 Web 站点的默认网站属性窗口,如果要设置用户对主页文件的读取权限,需要在____(2)____选项卡中进行配置。

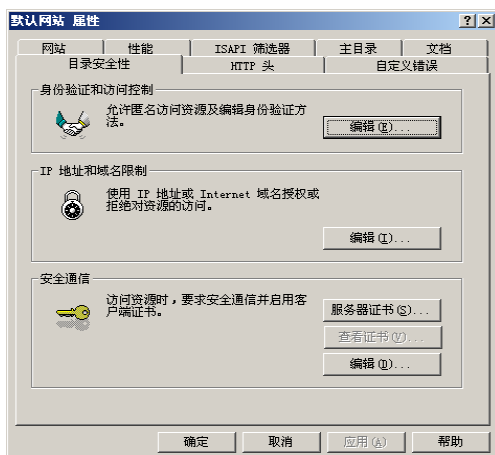


图 12-14 站点属性窗口

- (2) A. 网站 B. 主目录 C. 文档 D. HTTP 头

试题 3

配置 FTP 服务器的属性窗口如图 12-15 所示,默认情况下“本地路径”文本框中的值为____(3)____。

- (3) A. c:\inetpub\wwwroot B. c:\inetpub\ftproot
C. c:\wmpubi\wwwroot D. c:\wmpubi\ftproot

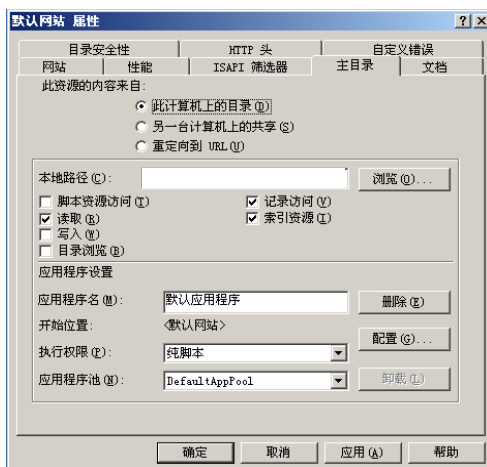


图 12-15 站点属性窗口

试题 4

在下列选项中,属于 IIS 6.0 提供的服务组件是____(4)____。

- (4) A. Samba B. FTP C. DHCP D. DNS

试题 5

IIS 6.0 将多个协议结合起来组成一个组件,其中不包括____(5)____。

- (5) A. POP3 B. SMTP C. FTP D. DNS

12.2.3 解析与答案

试题 1 分析

微软 IIS 服务是一项经典的 Web 服务，可以为广大用户提供信息发布和资源共享功能。身份认证是保证 IIS 服务安全的基础机制，IIS 支持以下 4 种 Web 身份认证方法。

① 匿名身份认证

如果启用了匿名访问，访问站点时，不要求提供经过身份认证的用户凭据。当需要让大家公开访问那些没有安全要求的信息时，使用此选项最合适。

② 基本身份认证

使用基本身份认证可限制对 NTFS 格式的 Web 服务器上文件的访问。使用基本身份认证，用户必须输入凭据，而且访问是基于用户 ID 的。用户 ID 和密码都以明文形式在网络间进行发送。

③ 摘要式身份认证

摘要式身份认证需要用户 ID 和密码，可提供中等的安全级别，如果用户要允许从公共网络访问安全信息，则可以使用这种方法。这种方法与基本身份认证提供的功能相同。摘要式身份认证克服了基本身份认证的许多缺点。在使用摘要式身份认证时，密码不是以明文形式发送的。

④ Windows 集成身份认证

Windows 集成身份认证比基本身份认证安全，而且在用户具有 Windows 域账户的内部网环境中能很好地发挥作用。在集成 Windows 身份认证中，浏览器尝试使用当前用户在域登录过程中使用的凭据，如果此尝试失败，就会提示该用户输入用户名和密码。如果用户使用集成 Windows 身份认证，则用户的密码将不传送到服务器。如果用户作为域用户登录到本地计算机，则此用户在访问该域中的网络计算机时不必再次进行身份认证。

试题 1 答案

(1) B

试题 2 分析

在 IIS 中，如果要设置用户对主页文件的读取权限，需要在主目录选项卡中进行配置。

试题 2 答案

(2) B

试题 3 分析

每个 FTP 站点也必须有一个主目录，默认为 c:\inetpub\ftproot。作为其他访问者访问用户 FTP 站点的起点。在 FTP 站点中，所有的文件都存放在作为根目录的主目录中，这就使其他访问者对用户 FTP 站点中的文件查找变得非常方便。

试题 3 答案

(3) B

试题 4 分析

IIS (Internet Information Server, 互联网信息服务) 是一种 Web (网页) 服务组件，其中包括 Web 服务器、FTP 服务器、NNTP 服务器和 SMTP 服务器，分别用于网页浏览、文件传输、新闻服务和邮件发送等方面。

试题 4 答案

(4) B

试题 5 分析

本试题考查考生对 IIS 6.0 组件的了解程度。

可以利用 Internet 信息服务器 (Internet Information Server, IIS) 来构建 WWW 服务器、FTP 服务器、SMTP 服务器和 POP3 服务器等。IIS 服务将 HTTP 协议、FTP 协议与 Windows Server 2000 出色的管理功能和安全特性结合起来, 提供了一个功能全面的软件包, 面向不同的应用领域给出了 Internet/Intranet 服务器解决方案。

试题 5 答案

(5) D

12.3 DNS 服务

在 DNS 这个考点中, 主要涉及三个方面的知识, 分别是 DNS 基础知识、Windows 系统下 DNS 服务器配置、Linux 系统下 DNS 服务器配置。

12.3.1 考点精讲

DNS 基础知识是对 DNS 的工作机制进行详细的解析, 作为网络工程人员是必须要熟悉这些内容的。

DNS 服务器的配置是服务器应用模块的一个知识点。通过配置服务器可以实现域名和 IP 地址之间的相互解析, 最终的结果是客户可以通过域名的方式去访问 Internet 上的公共服务器。

1. DNS 基础知识

下面简单介绍 DNS 的基础知识, 包括 DNS 服务器的分类, 以及相关的术语。

(1) DNS 服务器的类型

DNS 服务器可以分为主服务器、辅助域名服务器、高速缓存服务器、转换程序服务器 4 类。

① 主服务器

主服务器 (Primary Name Server) 是特定域所有信息的权威性信息源。它从域管理员构造的本地磁盘文件中加载域信息, 该文件 (区文件) 包含着该服务器具有管理权的一部分域结构的最精确信息。主服务器是一种权威性服务器, 因为它以绝对的权威去回答对其他域的任何查询。

配置主服务器需要一整套配置文件, 包括正向域的区域文件 (named.hosts) 和反向域的区文件 (named.rev)、配置文件 (named.conf)、高速缓存文件 (named.ca) 和回送文件 (named.local), 其他的配置都不需要这样一整套文件。

② 辅助域名服务器

辅助域名服务器 (Secondary Name Server) 可从主服务器中转移一整套域信息。区文件是从主服务器中转移出来的, 并作为本地磁盘文件存储在辅助服务器中。这种转移称为“区文件转移”。在辅助域名服务器中有一个所有域信息的完整备份, 可以权威地回答对该域的查询, 因此, 辅助域名服务器也称权威性服务器。

配置辅助域名服务器不需要生成本地区文件, 因为可以从主服务器中下载该区文件。然而其他的文件是需要的, 包括引导文件、高速缓存文件和回送文件。

③ 高速缓存服务器

高速缓存服务器 (Caching-only Server) 又称为唯高速缓存服务器, 可运行域名服务器

软件但是没有域名数据库软件。它从某个远程服务器取得每次域名服务器查询的回答，一旦取得一个答案，就将它放在高速缓存中，以后查询相同的信息时就用它予以回答。所有的域名服务器都按这种方式使用高速缓存中的信息，但唯高速缓存服务器则依赖于这一技术提供所有的域名服务器信息。唯高速缓存服务器不是权威性服务器，它提供的所有信息都是间接信息。

对于唯高速缓存服务器只需要配置一个高速缓存文件即可，但最常见的配置还包括一个回送文件，这或许是最常见的域名服务器配置。接着才是唯转换程序配置，它是最容易配置的。

④ 转换程序服务器

转换程序是一段要求域名服务器提供域信息的程序，在 Linux 系统中，它是作为一个库程序来实现的，不是一个单独的客户程序。在唯转换程序系统中，仅使用转换程序，并不运行域名服务器。这种系统是很容易配置的，最多只需要设置/etc/resolv.conf 文件即可。其他三个 BIND 配置选项都是用于 named 服务软件的。

(2) DNS 常用术语

DNS 是一个很复杂的概念，表 12-1 中列出了常用的 DNS 术语。

表 12-1 常用的 DNS 术语表

术 语	描 述
域	代表网络一部分的逻辑实体或组织
域名	主机名的一部分，代表包含这个主机的域，它可以和域交换使用
主机	有时也称为“节点”，网络上的一台计算机
域名服务器	提供 DNS 服务的计算机，它将 DNS 名字转化为 IP 地址
解析	把一个 DNS 服务器转化为与其相应的 IP 地址的过程
解析器	从域名服务器中提取 DNS 信息的程序或库子程序
反向解析	将给出的 IP 地址转化为与其相应的 DNS 名字
欺骗	使网络看上去好像具有不同的 IP 地址或域名的行为

DNS 区域：其实是一个数据库，它提供 DNS 名称和相关数据，例如 IP 地址或网络服务间的映射。

① 正向搜索区域：使得 DNS 服务器能够向前查找，对于 DNS 服务器，必须配置至少一个正向搜索区域，以便 DNS 服务器工作。

② 反向搜索区域：把计算机的 IP 地址映射到对用户友好的域名，反向搜索区域并不是必要的，正向区域也能够支持反向查找。

(3) DNS 服务器工作过程

当 DNS 客户机需要查询程序中使用的名称时，它会查询 DNS 服务器来解析该名称，客户机有时也可通过使用从以前查询获得的缓存信息中就地应答查询。DNS 服务器可使用其自身的资源记录信息缓存来应答查询，也可代表请求客户机来查询或联系其他 DNS 服务器，以完全解析该名称，并随后将应答返回至客户机，即递归查询。本地 DNS 服务器通过根提示，依次访问顶级域名服务器、二级域名服务器得到解析记录的过程则视为迭代查询。若本地 DNS 服务器通过转发器的方式得到解析记录的过程视为 DNS 服务器之间的递归查询。

DNS 查询的过程如图 12-16 所示。

一般情况下，DNS 客户服务要求服务器在返回应答前使用迭代过程来代表客户机完全解析名称。其迭代过程如图 12-17 所示。

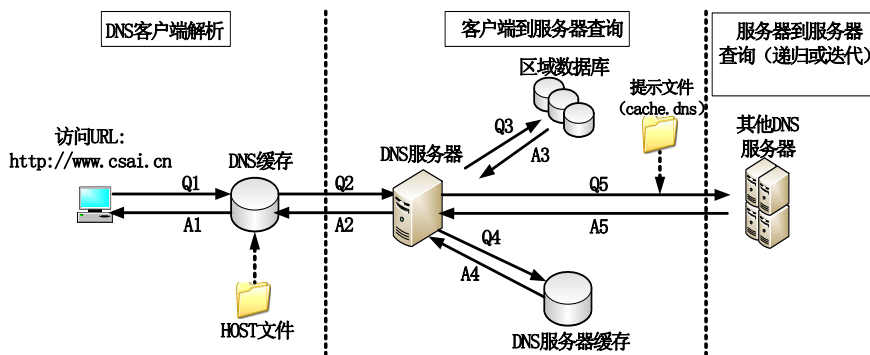


图 12-16 DNS 查询的过程

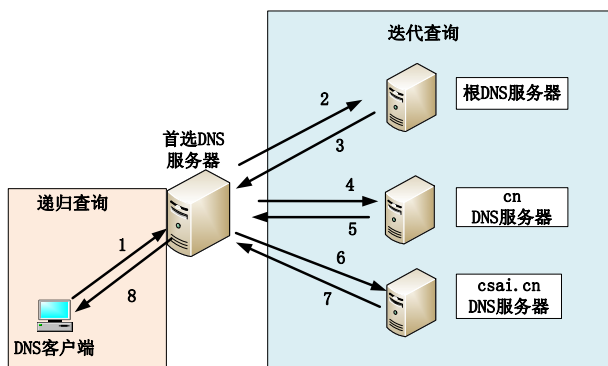


图 12-17 迭代解析过程

2. Windows 下 DNS 服务器配置

下面具体介绍在 Windows 系统下如何配置 DNS。

(1) 创建正向搜索区域

创建正向搜索区域的操作步骤如下。

① 打开“开始”菜单，选择“程序”→“管理工具”→“DNS”命令，打开 DNS 窗口，选择 DNS 服务器中“正向查找区域”标识。

② 选择管理器菜单中“操作”→“创建新区域”命令，系统启动“新建区域向导”对话框，单击“下一步”按钮，弹出“区域类型”界面，如图 12-18 所示。

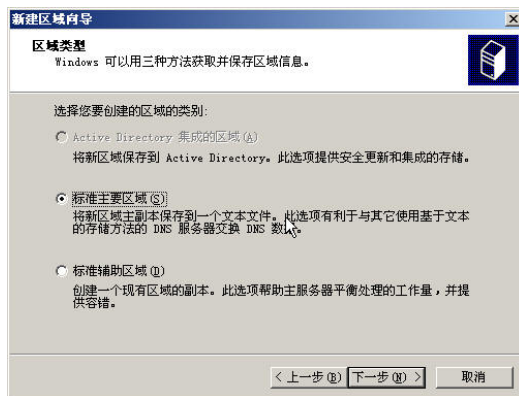


图 12-18 “区域类型”界面

③ 在图 12-18 中, 可以选择要创建区域类型对应的单选框, 在本例中选择“标准主要区域”单选框。单击“下一步”按钮, 弹出“区域名”界面, 如图 12-19 所示, 该对话框要求用户输入新建区域的名称。

④ 在图 12-19 中, 在“名称”文本框中输入新区域的名称。一般区域名在域名层次结构中区域所包含的最高域之后, 例如本例中输入 edu.csai.cn。单击“下一步”按钮, 弹出“区域文件”界面, 如图 12-20 所示。

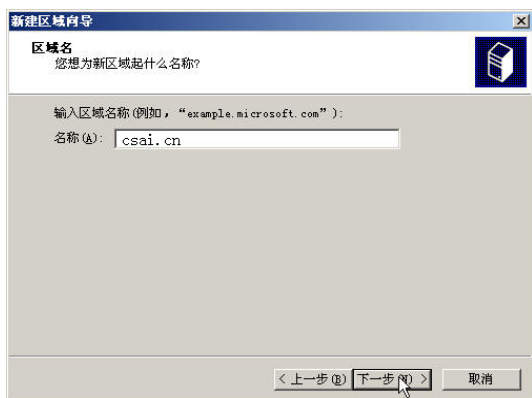


图 12-19 “区域名”界面

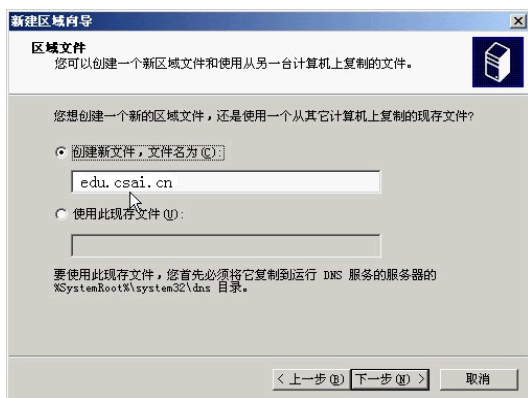


图 12-20 “区域文件”界面

⑤ 在图 12-20 中, 要求用户输入新 DNS 服务区域的数据库文件名。区域数据库文件名默认与区域名相同, 并以 dns 为扩展名, 如 edu.csai.cn.dns。当从另一台服务器移植区域时, 必须把现有文件存放到本计算机的 Winnt\System32\Dns 文件夹中。单击“下一步”按钮, 弹出“正在完成新建区域向导”界面, 该对话框显示出新区域的设置信息。如果信息正确, 单击“完成”按钮, 完成创建新区域的操作。在 DNS 窗口的右侧窗格中, 就显示出如图 12-21 所示的信息。

如果选择的是创建标准辅助区域, 输入标准辅助区域的区域名并单击“下一步”按钮后, 向导会要求输入“宿主服务器”的 IP 地址。用户既可以在“IP 地址”文本框中输入主 DNS 服务器的 IP 地址, 并单击“添加”按钮; 也可以单击“浏览”按钮, 选择主 DNS 服务器。

(2) 创建反向搜索区域

创建反向搜索区域的操作步骤如下。

① 打开“开始”菜单, 选择“程序”→“管理工具”→“DNS”命令, 打开 DNS 窗口, 选择 DNS 服务器中“反向查找区域”标识。

② 选择管理器菜单中“操作”→“创建新区域”命令, 系统启动“新建区域向导”对话框, 单击“下一步”按钮, 弹出“区域类型”界面, 如图 12-22 所示。

③ 选择“标准主要区域”单选框。单击“下一步”按钮, 弹出“网络 ID”对话框, 如图 12-23 所示。

④ 在图 12-23 中, 要求用户输入反向搜索区域的网络标识。例如, 在“网络 ID”文本框中输入 192.168.1, 表示网络中的所有反向搜索都在这个新区域中解析。图中反向搜索区域的区域名默认取自网络标识, 由反向 IP 地址加上 in-addr.arpa 后缀组成。单击“下一步”按钮, 弹出“区域文件”对话框, 如图 12-24 所示, 反向搜索区域的数据库文件名默认为区域名加上 dns 扩展名, 在这里使用系统的默认值。

⑤ 在图 10-24 中, 单击“下一步”按钮, 弹出“正在完成新建区域向导”界面, 对话框中显示出新区域的设置信息。单击“完成”按钮, 就完成了创建新区域的操作。

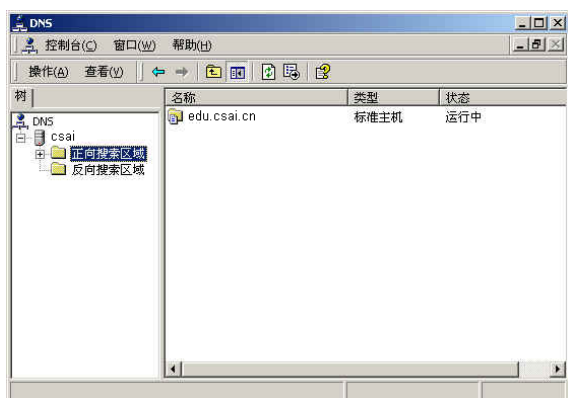


图 12-21 创建好的正向搜索区域

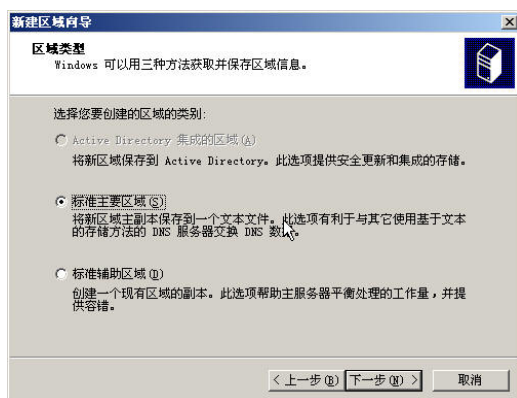


图 12-22 “区域类型”界面

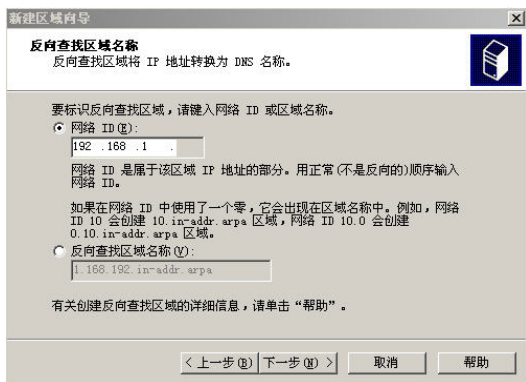


图 12-23 设置网络 ID

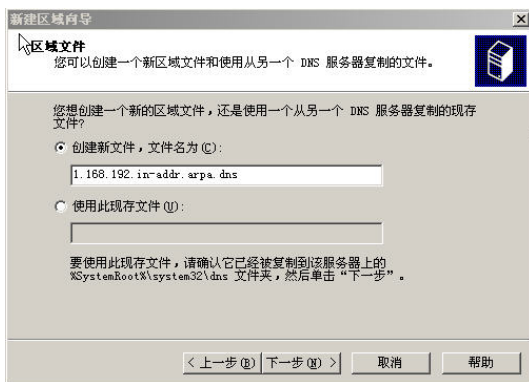


图 12-24 “区域文件”对话框

(3) 配置 DNS 服务

将 DNS 服务器添加到 DNS 控制台后, 就可以设置服务器的属性了, 比如只让 DNS 服务器侦听某些 IP 地址, 在不能解析名称时使用转发程序, 设置 DNS 服务器启动方法等。

配置 DNS 服务器属性的操作步骤如下。

① 在 DNS 控制台中选择想要配置属性的 DNS 服务器, 然后选择“操作”→“属性”命令, 打开如图 12-25 所示的 DNS 服务器属性对话框。

② 在默认情况下, DNS 服务器将侦听网络上所有配置为该服务器的 IP 地址的 DNS 通信信息。如果要将 DNS 限制为只侦听部分 IP 地址, 在服务器属性对话框的“接口”选项卡中选择“只在下列 IP 地址”单选框, 并在其下的“IP 地址”文本框中输入要侦听的 IP 地址, 然后单击“添加”按钮, 将 IP 地址添加到侦听 IP 地址列表中。当指定了侦听地址后, DNS 服务器将只侦听指定的 IP 地址, 为这些地址提供名称服务, 该功能大多用在 DNS 服务器计算机有多个 IP 地址的情况下。

如果 DNS 不能解析客户的名称请求, 可以启用转发程序。这样在 DNS 服务器不能应答查询时, 就将查询传送到指定的服务器中, 由该服务器协助解析。要启用转发程序, 可单击 DNS 服务器属性对话框中的“转发器”选项卡, 切换到“转发器”选项卡, 如图 12-26 所示。

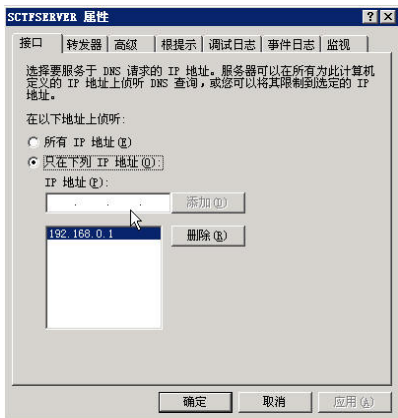


图 12-25 DNS 服务器属性对话框

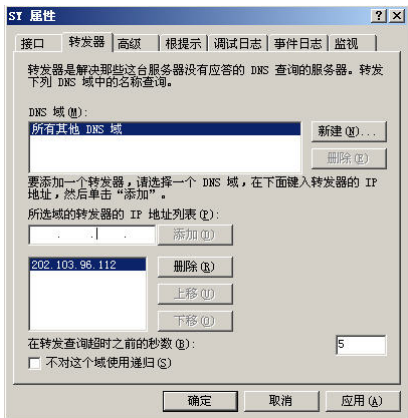


图 12-26 “转发器”选项卡

③ 在图 12-26 中，选择“转发器”选项卡，然后在“所选域的转发器的 IP 地址”文本框中输入转发 DNS 服务器的 IP 地址，并单击“添加”按钮将其添加到转发服务器列表中。通过在“在转发查询超时之前的秒数”文本框中输入以秒为单位的时间，还可以改变转发超时的时间。

④ 如果要设置 DNS 服务器寻找的其他 DNS 服务器，单击 DNS 服务器属性对话框中的“根提示”选项卡，如图 12-27 所示。单击“添加”按钮，并输入 DNS 服务器的名称与 IP 地址。

⑤ 因为启用调试日志记录会严重影响 DNS 服务器的性能，默认时，DNS 服务器关闭所有调试日志记录。用户可以手工启用某些调试日志记录，只要打开 DNS 服务器属性对话框中的“日志”选项卡，并在“调试日志记录选项”列表框中选择要调试的日志记录即可，如图 12-28 所示。



图 12-27 “根提示”选项卡

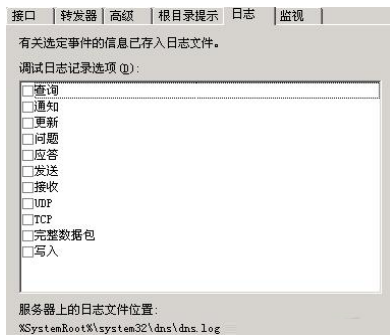


图 12-28 “日志”选项卡

3. Linux 下 DNS 服务器配置

BIND 称为转换程序（resolver），它产生域名信息的查询，将这类信息发送给服务器，DNS 软件回答转换程序的查询。BIND 的服务方面是一个称为 named 的守护进程。3 种基本 BIND 配置任务包括：配置 BIND 转换程序、配置 BIND 域名服务、建立服务器数据库文件。

服务器数据库文件，又称为“区域文件（zone file）”。“区域”是指域数据库文件，是域数据库文件中包含域信息的集合，包含域信息的文件称为“区域文件”。

(1) host.conf 文件解析

/etc/host.conf 是用来控制本地转换程序的文件设置的。该文件告诉转换程序使用哪些服务，按照什么顺序进行。该文件的字段可以用空格或制表符分隔。字符“#”表示注释行。如表 12-2 所示是可在 host.conf 中指定的选项。

表 12-2 /etc/host.conf 文件的配置选项

选 项	说 明
order	指定按照哪种顺序来尝试不同的名字解析机制。按列出的顺序来进行指定的解析服务。支持下面的名字解析机制： hosts 试图通过查找本地/etc/hosts 文件来解析名字 bind 使用 DNS 域名服务器来解析名字 nis 使用网络信息服务（NIS）协议来解析主机名字
multi	以 off 和 on 为参数。与 host 查询一起使用，用来确定一台主机是否在/etc/hosts 文件中指定了多个 IP 地址
nospoof	如果用逆向解析找出与指定的地址匹配的主机名，对返回的地址进行解析以确认它确实与你查询的地址相配。为了防止“骗取”IP 地址，通过指定 nospoof on 来允许这种功能
alert	以 off 和 on 为参数。如果打开，任何试图骗取 IP 地址的行为都通过 syslog 工具进行记录
trim	以域名为参数。在/etc/hosts 中查找名字前，trim 删除这个域名。使你只把基本主机名放在 /etc/host.conf 中而不指定域名

下面这个例子是主机 vlager 上的/etc/host.conf 文件。

```
# /etc/host.conf
# We have named running, but no NIS (yet)
order bind hosts
# Allow multiple addrs
multi on
# Guard against spoof attempts
nospoof on
# Trim local domain (not really necessary).
trim csai.cn.
```

这个例子给出了域 csai.cn 的通用解析程序配置。该解析程序首先使用 DNS，然后使用 /etc/hosts 文件查找主机名。在解析查找中指定本地/etc/hosts 文件是一个可靠的选择。如果由于某种原因不能使用域名服务器，还可以使用主机文件中列出的那些主机名。

(2) resolv.conf 文件解析

当配置转换程序使用 BIND 域名服务查询主机时，我们必须告诉转换程序使用哪一个域名服务器。用来完成这项任务的工具就是/etc/resolv.conf 文件。/etc/resolv.conf 控制转换程序使用 DNS 解析主机名使用的方式，它可以明确地定义系统的配置，允许我们命名由于默认服务器不响应而使用的备份服务器。在/etc/resolv.conf 中使用的命令，具有系统专用的形式，但一般都支持 nameserver 和 domain 两项命令。

① nameserver 项：利用 IP 地址让转换程序去识别查询域信息的那些服务器。我们可以多次使用 nameserver 选项，可以使用多达 3 个域名服务器。这些域名服务器是按照它们在文件中的顺序进行查询的，如果没有接收到一个服务器的响应，就去尝试表中的下一个服务器，直到所有服务器试完为止（如果在/etc/resolv.conf 文件中设置了 3 个以上的域名服务器，那么，即使前 3 个服务器都没有响应查询请求，Linux 也不会去请求后面的服务器）。我们应该将最可靠的域名服务器列在最前面，以便在查询时不会超时。

② domain 项：用来定义默认域名（主机的本地域名）。转换程序会将默认域名挂在任

何不含点的主机名后面。例如，转换程序接收到主机名 `vale`（它不含点），就将其默认域名挂接在 `vale` 后面，构成对它的查询。如果 `domian` 域中的 `name` 值是 `csai.cn`，那么转换程序就将查询 `vale.csai.cn`。看一看下面这个例子，这是 `Virtual Brewery` 中的 `resolv.conf` 文件。

```
# /etc/resolv.conf
# Our domain
domain csai.cn
# We use vlager as central nameserver:
nameserver 191.72.1.1
```

在该例中，通过 `domain` 指定默认域名，并列出一个用于解析主机名的域名服务器。在这个例子中没有指定查询顺序（使用 `search` 选项），因此如果要查询一台机器的地址（如 `vale`），解析器则首先试图查找 `vale`，如果没找到，则查找 `vale.csai.cn`，然后再查找 `csai.cn`。

（3）设置域名服务器

在 `Linux` 上的域名服务是由 `named` 进程来执行的，该进程从被称做 `/etc/named.conf` 的配置文件获取有关信息和将主机名映射为 `IP` 地址的各种文件。为了运行 `named`，只要在命令行中输入：`# /etc/rc.d/init.d/named start` 即可。

虽然转换程序的配置只需要一个配置文件，但是在配置 `named` 时却要使用多个文件，一整套 `named` 配置文件如表 12-3 所示。

表 12-3 named 配置文件

配 置 文 件	说 明
<code>named.conf</code>	设置一般的 <code>named</code> 参数，指向该服务器使用的域数据库信息的源，这类源可以是本地磁盘文件或远程服务器
<code>named.ca</code>	指向根域名服务器
<code>named.local</code>	用于在本地转换回送地址
<code>Named.hosts</code>	将主机名映射为 <code>IP</code> 地址
<code>Named.rev</code>	用于反向域的、将 <code>IP</code> 地址映射到主机名的区文件

`named.conf` 文件通常很小，只包括一些指向 `DNS` 信息源的信息。其中某些源是本地文件，其他则是远程服务器的。下面举一个需要生成的每种文件类型的例子。表 12-4 概括了 `named.conf` 文件中使用的各种配置语句，它提供的信息能帮助我们了解这些例子。

表 12-4 named.conf 文件的配置选项

选 项	说 明
<code>Directory</code>	指定 <code>DNS</code> 文件所在的目录。可以重复此选项，以指定几个不同的目录。可以给出这些目录相关的文件路径名
<code>Master</code>	以一个域名和一个文件名为参数。此选项声明 <code>named</code> 对指定的域具有控制权，并使 <code>named</code> 从指定的区域加载信息
<code>Hint</code>	为 <code>named</code> 建立高速缓存信息。以一个域名和一个文件名为参数。域名通常用“.”指定。指定的文件包括一组称为服务器提示的记录，这些记录列出了根域名服务器的信息
<code>Forwarders</code>	以一个域名服务器的列表作为参数。告诉本地域名服务器：如果它不能从它的本地信息中解析出地址，那么就与该列表中的服务器联系
<code>Slave</code>	把本地域名服务器变成一个从属服务器。如果给出了此选项，那么本地服务器就试着通过递归查询来解析 <code>DNS</code> 名字。它只把请求传递给 <code>forwarders</code> 选项行列出的服务器中的一个

配置 `named.conf` 文件所使用的方法，是用来控制将域名服务器作为主服务器、辅助服务器还是唯高速缓存服务器的。理解不同配置的最佳方法，是讨论各种 `named.conf` 的示例

文件。

(4) 唯高速缓存服务器

配置唯高速缓存域名服务器是很简单的，必须有 `named.conf` 和 `named.ca` 文件，通常也要用到 `named.local` 文件。下面是用于唯高速缓存服务器的 `named.conf` 文件的例子，其中以“//”开头的是注释：

```
// generated by named-bootconf.pl
options {
    directory "/var/named";
}
/*
 * If there is a firewall between you and nameservers you want
 * to talk to, you might need to uncomment the query-source
 * directive below. Previous versions of BIND always asked
 * questions using port 53, but BIND 8.1 uses an unprivileged
 * port by default.
 */
// query-source address * port 53;
};
// a caching only nameserver config
zone "."{
    type hint;
    file "named.ca";
};
zone "0.0.127.in-addr.arpa"{
    type master;
    file "named.local";
};
```

`directory` 这一行告诉 `named` 到哪里去寻找文件。所有其后命名的文件都将是相对于此目录的。该文件告诉 `named` 去维持一个域名服务器响应的高速缓存，并利用 `named.ca` 文件的内容去初始化该高速缓存。该高速缓存初始化文件的名称可以是任何名称，但一般使用 `/var/named/named.ca`。在实际中，几乎每一种服务器的配置都应该附加高速缓存服务器功能。

但是，在我们这个例子中却有一个 `master` 语句。事实上，几乎在每一个唯高速缓存的配置文件中都有这个语句，它将本地服务器定义为它自己的回送域的主服务器，并假定该域的信息存储在 `named.local` 文件中。这个回送域是一个 `in-addr.arpa` 域（`in-addr.arpa` 域用于指定逆向解析，或 IP 地址到 DNS 名称解析），它将地址 `127.0.0.1` 映射为名称 `localhost`。转换自己的回送地址对于大多数人都是有意义的，因为大多数的 `named.conf` 文件都包含这一项。

在大多数唯高速缓存服务器的配置文件中，这种 `directory`、`master` 和 `hint` 语句是唯一使用的语句，但也可以增加其他的语句，如 `forwarders` 和 `slave` 等语句都可以使用。

(5) 主服务器和辅助服务器的配置

虚构一个 `csai.cn` 的域名，用来举例说明主服务器和辅助服务器的基础。下面是将 `vlager` 定义为 `csai.cn` 域的主服务器的 `named.conf` 文件。

```
// generated by named-bootconf.pl
options {
    directory "/var/named";
}
/*
 * If there is a firewall between you and nameservers you want
 * to talk to, you might need to uncomment the query-source
 * directive below. Previous versions of BIND always asked
 * questions using port 53, but BIND 8.1 uses an unprivileged
 * port by default.
 */
// query-source address * port 53;
```

```

};
// a caching only nameserver config
zone "."{
type hint;
file "named.ca";
};
zone "csai.cn"{
type master;
file "named.hosts";
};
zone "0.0.127.in-addr.arpa" {
type master;
file "named.local";
};
zone "72.191.in-addr.arpa"{
type master;
file "named.rev";
};
};

```

上例中第一个 **master** 告诉我们这是 **csai.cn** 域的主服务器。该域的数据是从 **named.hosts** 文件中加载的。在这个例子中，我们将文件名 **named.hosts** 作为区文件名，但也可以使用更有说明性的文字，例如，**csai.cn** 区域文件的名称使用 **csai.cn.hosts** 则较好。

第三个 **master** 语句指向能将 IP 地址 191.72.0.0 映射为主机名的文件。它假定本地服务器是反向域 **72.191.in-addr.arpa** 的主服务器，该域的数据从文件 **named.rev** 中加载。

在上例配置中的 **hint** 语句和第二个用于回送域的 **primary** 语句，我们前面在唯高速缓存配置中已经讨论过。在这些配置中，它们的作用是相同的，而且几乎在任何配置中都要使用它们。

辅助服务器的配置与主服务器的配置不同，它使用 **slave** 语句代替 **master** 语句。**slave** 语句指向用作域信息源的远程服务器，以替代本地磁盘文件。下面的 **named.conf** 文件可以将 **vale** 配置成 **vbrew.com** 域的辅助服务器。

```

// generated by named-bootconf.pl
options {
directory "/var/named";
/*
* If there is a firewall between you and nameservers you want
* to talk to, you might need to uncomment the query-source
* directive below. Previous versions of BIND always asked
* questions using port 53, but BIND 8.1 uses an unprivileged
* port by default.
*/
// query-source address * port 53;
};
// a caching only nameserver config
zone "." {
type hint;
file "named.ca";
};
zone "0.0.127.in-addr.arpa" {
type master;
file "named.local";
};
};
zone "csai.cn"{
type slave;
file "named.hosts";
masters { 191.72.1.3;};
};
zone "72.191.in-addr.arpa"{

```

```

type slave;
file "named.rev";
masters {191.72.1.3;};
};
cache.named.ca
secondary vbrew.com 191.72.1.3 named.hosts
secondary 72.191.in-addr.arpa 191.72.1.3 named.rev
primary 0.0.127.in-addr.arpa named.local

```

第一个 slave 语句是使这个服务器成为 csai.cn 的辅助服务器。它告诉 named 从 IP 地址为 191.72.1.3 的服务器中下载 csai.cn 的信息，并将其数据保存在/var/named/named.hosts 文件中。

下一行表示该本地服务器也是反向域 72.191.in-addr.arpa 的一个辅助服务器，而且该域的数据也从 191.72.1.3 中下载。该反向域的数据存储在/var/named/ named.rev 中。

(6) DNS 数据库文件和资源记录

配置 named 所需的所有文件（域名.zone、网络 ID.rev、localhost.zone 和 named.ca）中的信息是以称为资源记录的形式存在的。每个资源记录都有一个类型，这个类型说明记录的功能。这些记录都是标准资源记录，称为 RR（Resource Records）。表 12-5 中列出了最常见的资源记录类型。

表 12-5 最常见的资源记录类型

资源记录名	记 录 类 型	功 能 说 明
地址	A	将主机名转换为地址。这个字段保存以点分隔的十进制数形式的 IP 地址。任何给定的主机都只能有一个 A 记录，因为这个记录被认为是授权信息。这个主机的任何附加地址名或地址映射必须用 CNAME 类型给出
别名	CNAME	给定一个主机的别名，主机的规范名字是在这个主机的 A 记录中指定的
主机信息	HINFO	描述主机的硬件和操作系统
邮件交换	MX	建立邮件交换器记录。MX 记录告诉邮件传送进程把邮件送到另一个系统，这个系统知道如何将它递送到它的最终目的地
域名服务器	NS	标识一个域的域名服务器。NS 资源记录的数据字段包括这个域名服务器的 DNS 名。我们还需要指定这个名字服务器的地址与主机名相匹配的 A 记录
指针	PTR	将地址变换成主机名。主机名必须是规范主机名
管理开始	SOA	告诉域名服务器它后面跟着的所有资源记录是控制这个域的（SOA 表示授予控制权）。其数据字段用括号括起来并且通常是多行字段

12.3.2 一点一练

试题 1

在 Linux 中，在 DNS 客户端上指定 DNS 服务器的配置文件是____(1)____。

- (1) A. /etc/hostname B. /etc/host.conf C. /etc/resolv.conf D. /etc/httpd.conf

试题 2

DNS 服务器中提供了多种资源记录，其中____(2)____定义了区域的邮件服务器及其优先级。

- (2) A. SOA B. NS C. PTR D. MX

试题 3

在 Windows 系统中，进行域名解析时，客户端系统会首先从本机的____(3)____文件中寻找域名对应的 IP 地址。在该文件中，默认情况下必须存在的一条记录是____(4)____。

- (3) A. hosts B. lmhosts C. networks D. dnsfile

- (4) A. 192.168.0.1 gateway B. 224.0.0.0 multicast
C. 0.0.0.0 source D. 127.0.0.1 localhost

试题 4

DNS 服务器在名称解析过程中正确的查询顺序为____(5)_____。

- (5) A. 本地缓存记录→区域记录→转发域名服务器→根域名服务器
B. 区域记录→本地缓存记录→转发域名服务器→根域名服务器
C. 本地缓存记录→区域记录→根域名服务器→转发域名服务器
D. 区域记录→本地缓存记录→根域名服务器→转发域名服务器

试题 5

DNS 服务器进行域名解析时，若采用递归方法，发送的域名请求为____(6)_____。

- (6) A. 1 条 B. 2 条 C. 3 条 D. 多条

12.3.3 解析与答案

试题 1 分析

/etc/resolv.conf: 该文件是 DNS 域名解析的配置文件，它的格式很简单，每行以一个关键字开头，后接配置参数。resolv.conf 的关键字主要有 4 个，具体介绍如下。

- ① Nameserver: 定义 DNS 服务器的 IP 地址。
- ② Domain: 定义本地域名。
- ③ Search: 定义域名的搜索列表。
- ④ Sortlist: 对返回的域名进行排序。

当系统中同时存在 DNS 域名解析和/etc/hosts 主机表机制时，由该/etc/host.conf 确定主机名解释顺序。

试题 1 答案

- (1) C

试题 2 分析

在管理域名时，需要用到 DNS 资源记录。DNS 资源记录是域名解析系统中基本的数据元素。每个记录都包含一个类型，一个生存时间，一个类别以及一些跟类型相关的数据。在设定 DNS 域名解析、子域名管理、E-mail 服务器设定以及进行其他域名相关的管理时，需要使用不同类型的资源记录。

- ① A 记录代表“主机名称”与“IP”地址的对应关系，作用是把名称转换成 IP 地址。
- ② CNAME 记录代表别名与规范主机名称之间的对应关系。
- ③ MX 记录提供邮件路由信息：提供网域的“邮件交换器”(Mail Exchanger)的主机名称以及相对应的优先级。
- ④ PTR 记录代表“IP 地址”与“主机名”的对应关系，作用刚好与 A 记录相反。
- ⑤ NS 记录用于标识区域的 DNS 服务器，即指负责此 DNS 区域的权威名称服务器，用哪一台 DNS 服务器来解析该区域。

试题 2 答案

- (2) D

试题 3 分析

在 Windows 系统中，进行域名解析时，客户端系统会首先从本机的 hosts 文件中寻找域名对应的 IP 地址。hosts 文件是用于本地 DNS 服务的，采用 IP 域名的格式写在一个文本文件中，Windows 系统上一般存放在系统盘的 system32 目录下，例如“C:\windows\system32\

drivers\etc\”，本地主机一般都被定义为“127.0.0.1 localhost”。

试题 3 答案

(3) A

(4) D

试题 4 分析

DNS 服务器在名称解析过程中首先查找区域记录，然后查找本地缓存记录，如果还找不到就转向转发域名服务器，转发域名服务器负责非本地域名的域名查询，最后转向根域名服务器。

试题 4 答案

(5) B

试题 5 分析

主机向本地域名服务器的查询一般都是采用递归查询。所谓递归查询就是：如果主机所询问的本地域名服务器不知道被查询域名的 IP 地址，那么本地域名服务器就以 DNS 客户的身份，向其他根域名服务器继续发出查询请求报文（即替该主机继续查询），而不是让该主机之间进行下一步的查询。因此，递归查询返回的查询结果或者是所要查询的 IP 地址，或者是报错，表示无法查询到所需的 IP 地址。

试题 5 答案

(6) A

12.4 DHCP 服务

在 DHCP 服务这个考点中，主要涉及三个方面的知识，分别是 DHCP 基础知识、Windows 系统下 DHCP 服务器配置、Linux 系统下 DHCP 服务器配置。

12.4.1 考点精讲

DHCP 基础知识是对 DHCP 的工作机制进行详细的解析，作为网络工程人员是必须要熟悉这些内容的。

DHCP 服务器的配置是服务器应用模块的一个知识点。通过配置 DHCP 服务器可以实现网络中 IP 地址的自动分配，大大节约网络工程师的操作成本，提高了工作效率。DHCP 服务目前在企业中使用非常广泛。

1. DHCP 服务基础知识

配置 DHCP 服务器有如下优点。

① 管理员可以集中为某网段指定通用和特定子网的 TCP/IP 参数，并且可以定义使用保留地址的客户机的参数。

② 客户机无须手工配置 TCP/IP，提供安全可信的配置。DHCP 避免了在每台计算机上手工输入数值引起的配置错误，还能防止网络上计算机配置地址的冲突。

③ 使用 DHCP 服务器能大大减少配置花费的开销和重新配置网络上计算机的时间，服务器可以在指派地址租约时配置所有的附加配置值。

④ 客户机在子网间移动时，旧的 IP 地址自动释放以便再次使用。再次启动客户机时，DHCP 服务器会自动为客户机重新配置 TCP/IP。

⑤ 大部分路由器可以转发 DHCP 配置请求，因此，互联网的每个子网并不都需要 DHCP 服务器。

DHCP 是基于客户机-服务器模型设计的，DHCP 客户机和 DHCP 服务器之间通过收发 DHCP 消息进行通信，如图 12-29 所示。

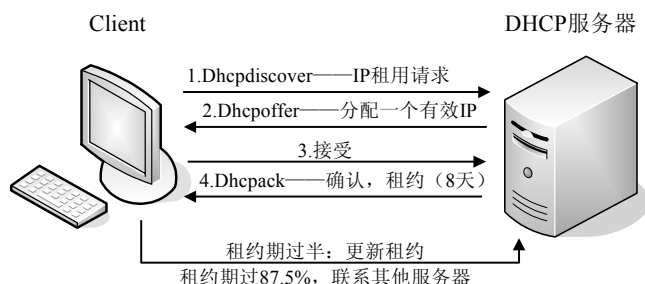


图 12-29 DHCP 服务过程

不论是 DHCP 客户机还是 DHCP 服务器，都是通过按 DHCP 消息格式要求来填写各个段的，形成具体的 DHCP 消息，DHCP 使用的传输协议是非面向连接的 UDP（用户数据报协议），从 DHCP 客户机发出的 DHCP 消息送往 DHCP 服务器的端口 67，DHCP 服务器发给客户机的 DHCP 消息送往 DHCP 客户机的端口 68，由于在取得服务器赋予的 IP 之前，DHCP 客户机并没有自己的 IP，所以包含 DHCP 消息的 UDP 数据报的 IP 头的源地址段是 0.0.0.0，目的地址则是 255.255.255.255。

关于 IP 地址租约的问题，需要注意的是当 DHCP 客户机租期达 50% 时，重新更新租约，客户机发送 DHCPRequest 包。当租约达到 87.5% 时，进入重新申请状态，客户机发送 DHCPDiscover 包。

DHCP 服务器有以下 3 种为 DHCP 客户机分配 TCP/IP 地址的方式。

① 手工分配：管理员在 DHCP 服务器上通过手工方法配置 DHCP 客户机的 IP 地址。当 DHCP 客户机要求网络服务时，DHCP 服务器把手工配置的 IP 地址传递给 DHCP 客户机。

② 自动分配：不需要进行任何的 IP 地址手工分配。当 DHCP 客户机第一次向 DHCP 服务器租用 IP 地址后，这个地址就永久地分配给了该 DHCP 客户机，而不会再分配给其他客户机。

③ 动态分配：当 DHCP 客户机向 DHCP 服务器租用 IP 地址时，DHCP 服务器只是暂时分配给客户机一个 IP 地址。只要租约到期，这个地址就会还给 DHCP 服务器，以供其他客户机使用。如果 DHCP 客户机仍需要一个 IP 地址来完成工作，则可以再要求另外一个 IP 地址。

2. Windows 下 DHCP 配置

完成安装 DHCP 服务器的操作后，用户在 DHCP 控制台窗口中，将看到添加服务器的图标、服务器的名称及地址，如图 12-30 所示。

（1）创建 DHCP 作用域

创建作用域的主要作用就是为服务器指定和配置好可分配的 IP 地址。因此，在创建新的 DHCP 服务器的操作中，创建作用域的工作是至关重要的，它关系到 DHCP 是否拥有可分配的 IP 地址。

创建 DHCP 作用域的操作步骤如下。

① 选择“开始”→“程序”→“管理工具”→“DHCP”命令，打开 DHCP 控制台窗口。选择要创建作用域的 DHCP 服务器，选择“操作”→“新建作用域”命令，弹出“新建作用域向导”对话框“作用域名”界面，如图 12-31 所示。作用域名能帮助用户快速识别有关的 IP 地址。

② 单击“下一步”按钮，弹出“IP 地址范围”界面，如图 12-32 所示。

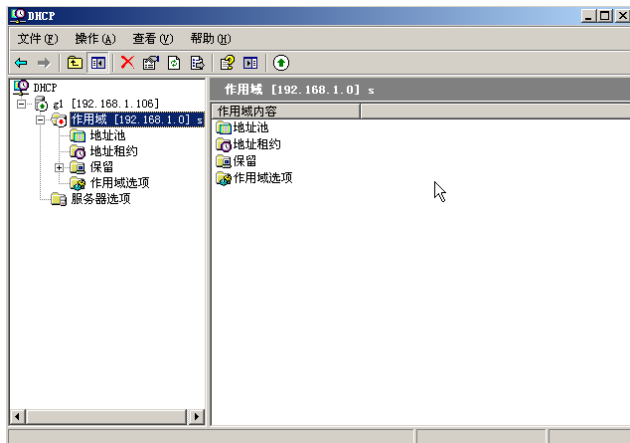


图 12-30 添加服务器后的 DHCP 控制台

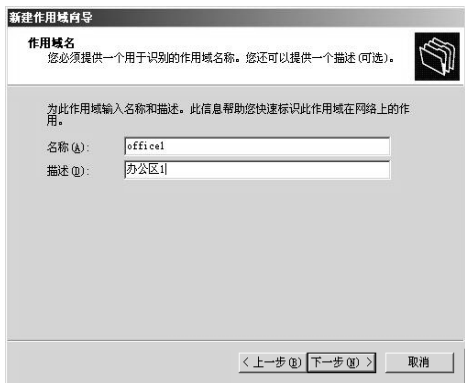


图 12-31 “作用域名”界面

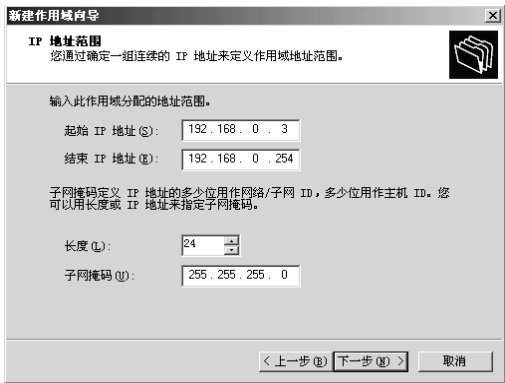


图 12-32 “IP 地址范围”界面

③ 在图 12-32 中，可以指定作用域的地址范围及子网掩码。DHCP 管理器会为用户提供一个适用于大多数网络的默认子网掩码。如果该默认值不正确，可以在“长度”或“子网掩码”文本框中输入正确的值。单击“下一步”按钮，弹出“添加排除”界面，如图 12-33 所示。

④ 在图 12-33 中，可以定义服务器不分配的 IP 地址范围。排除范围应包括所有手工分配给其他 DHCP 服务器、非 DHCP 客户端等。单击“下一步”按钮，进入“租约期限”界面，如图 12-34 所示。

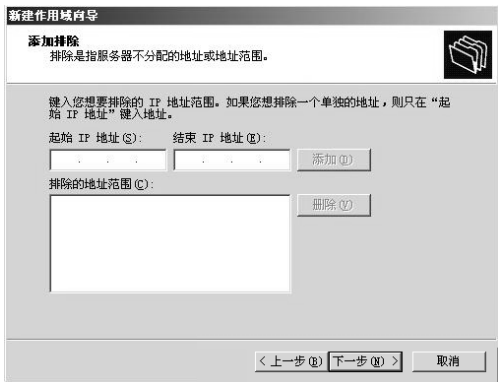


图 12-33 “添加排除”界面

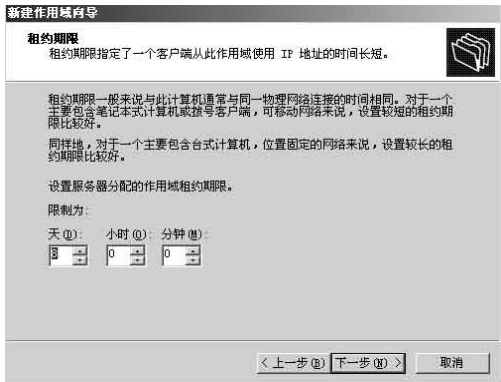


图 12-34 “租约期限”界面

⑤ 在图 12-34 中，租约期限指定了客户机使用 DHCP 服务器所分配的 IP 地址的时间。要想让网络客户使用作用域，必须配置最常用的 DHCP 选项，这些选项包括网关、DNS 服务器和 WINS 设置等。单击“下一步”按钮，弹出“路由器（默认网关）”界面，如图 12-35 所示。

⑥ 在图 12-35 中，要求用户配置作用域的网关（或路由器）。单击“下一步”按钮，弹出“域名称和 DNS 服务器”对话框，如图 12-36 所示，DNS 服务器用来把域名转换成 IP 地址。



图 12-35 “路由器（默认网关）”界面

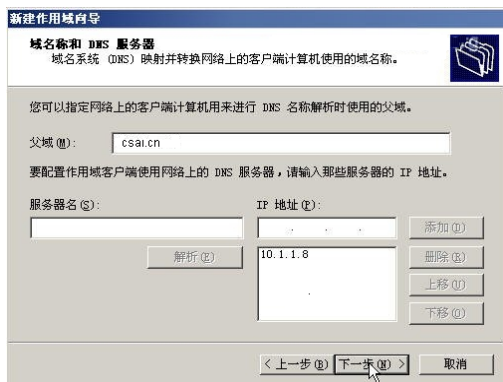


图 12-36 “域名称和 DNS 服务器”界面

⑦ 在图 12-36 中，在“父域”文本框中输入域名，在“服务器名”文本框中输入服务器的名称，然后单击“解析”按钮，则在右侧的“IP 地址”中显示出该服务器名称所对应的 IP 地址。单击“下一步”按钮，弹出“WINS 服务器”界面，在该界面中输入 WINS 服务器地址，WINS 服务器可以将 Windows 客户的计算机名称转换成相应的 IP 地址。在“服务器名”文本框中输入 WINS 服务器的名称，单击“解析”按钮，则在右侧的 IP 文本框中显示出该服务器名称所对应的 IP 地址，如图 12-37 所示。

⑧ 在图 12-37 中，单击“下一步”按钮，弹出“激活作用域”界面，如图 12-38 所示。

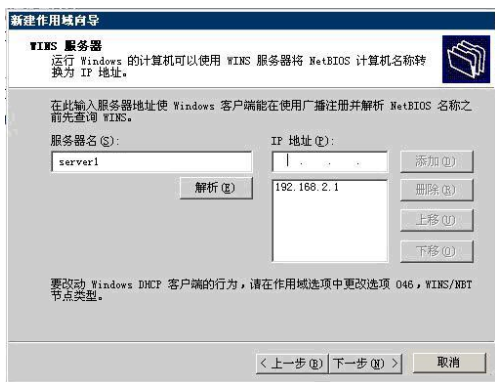


图 12-37 “WINS 服务器”界面



图 12-38 “激活作用域”界面

⑨ 在图 12-38 中，选择“是，我想现在激活此作用域”单选框。最后单击“完成”按钮，关闭“新建作用域向导”对话框，在 DHCP 控制台上就列出了刚才所创建的作用域，如图 10-39 所示。

（2）DHCP 中继代理

Windows 服务器系统内置的中继代理功能，完全可以将原先的 DHCP 服务器利用起来，

分别为多个不同子网提供 IP 地址分配服务。下面以一台 DHCP 服务器同时为两个子网提供地址分配服务为例来详细介绍如何启用 DHCP 中继代理程序,协助不同子网中的工作站完成跨子网申请 IP 地址的任务。

① 配置虚拟路由

在启用 DHCP 中继代理功能之前,需要先将工作站配置成一个虚拟的路由器,以便利用该路由器将局域网中的两个不同子网连接起来。Windows 系统在默认状态下没有启用路由和远程访问服务,因此我们必须先用手工方法来安装并配置好该服务。

a. 打开系统控制面板窗口中的“管理工具”窗口,再双击“路由和远程访问”项目,打开如图 12-40 所示的“路由和远程访问”窗口。

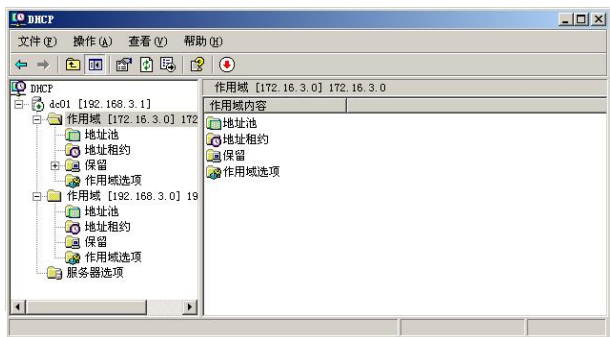


图 10-39 新建的作用域

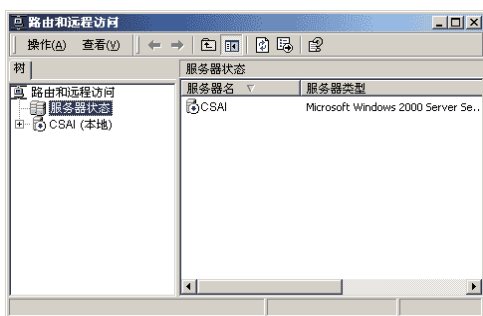


图 12-40 “路由和远程访问”窗口

b. 在图 12-40 中,右击本地计算机图标,从弹出的快捷菜单中选择“配置并启用路由和远程访问”命令,打开“路由和远程访问服务器安装向导”对话框,单击该窗口中的“下一步”按钮,进入到如图 12-41 所示的向导配置界面。

c. 在图 12-41 中,选中“自定义配置”单选框,再单击“下一步”按钮,在其后出现的向导窗口中选中“LAN 路由”复选框,如图 12-42 所示。

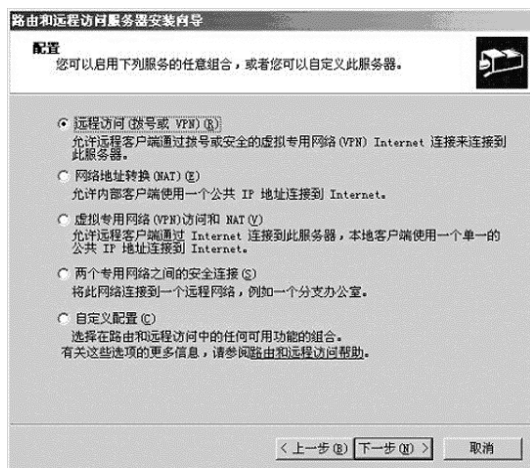


图 12-41 向导配置界面

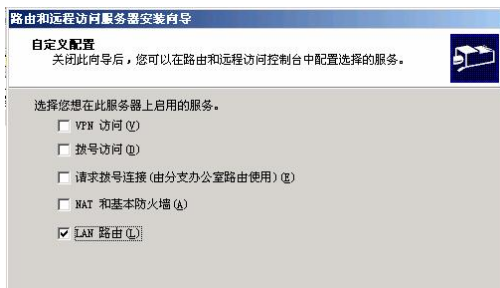


图 12-42 选中“LAN 路由”复选框

d. 单击“完成”按钮,退出路由和远程访问服务器安装向导窗口。

② 启用 DHCP 中继代理

所谓“中继代理”,其实就是为处于不同子网中的工作站与服务器之间中转传输

BOOTP/DHCP 消息的一种特殊程序，为了实现 DHCP 中继代理功能，需要配置一个 DHCP 中继代理服务器。位于同一子网中的工作站以广播方式申请 IP 地址时，DHCP 中继代理服务器就会自动将 IP 地址申请信息中转传输到位于另外一个子网中的 DHCP 服务器，DHCP 服务器再将 IP 地址应答信息通过中继代理服务器转发给指定的工作站，从而协助工作站完成跨子网申请 IP 地址服务。系统在默认状态下并没有安装 DHCP 中继代理程序，因此必须先将 DHCP 中继代理程序安装好。

- a. 进入如图 12-40 所示的“路由和远程访问”窗口，然后逐一展开该界面左侧区域的“本地计算机”→“IP 路由选择”→“常规”选项。再右击“常规”选项，从弹出的快捷菜单中选择“新增路由协议”命令，打开如图 12-43 所示的“新路由协议”对话框。
- b. 在图 12-43 中，选中“路由协议”列表框中的“DHCP 中继代理程序”选项，再单击“确定”按钮结束 DHCP 中继代理程序的安装操作。
- c. 指定 DHCP 服务器，右击前面已经安装好的“DHCP 中继代理程序”项目，在弹出的快捷菜单中选择“属性”命令，打开如图 12-44 所示的“DHCP 中继代理程序属性”对话框。



图 12-43 “新路由协议”对话框

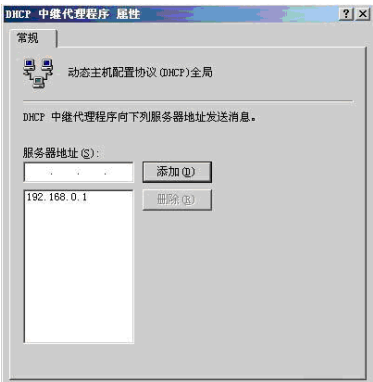


图 12-44 “DHCP 中继代理程序属性”对话框

在“常规”选项卡中，将位于另外一个子网的 DHCP 服务器 IP 地址准确地填写在此处的“服务器地址”文本框中，例如，DHCP 服务器 IP 地址是“192.168.1.55”，再单击“添加”按钮，完成 DHCP 服务器的指定工作；如果局域网中包含多个 DHCP 服务器，则可以分别将这些 DHCP 服务器的 IP 地址添加到这里。

完成上面的各项工作后，DHCP 中继代理程序现在还不能立刻发挥作用，还必须对其访问接口进行配置。在配置 DHCP 中继代理程序的访问接口时，需要先进入路由和远程访问界面。

③ 添加 DHCP 中继代理端口

- a. 展开“路由和远程访问”界面中左侧区域的“本地计算机”→“IP 路由选择”→“DHCP 中继代理程序”选项，再用鼠标右键单击“DHCP 中继代理程序”选项，从弹出的快捷菜单中选择“新增接口”命令，如图 12-45 所示。
- b. 打开中继代理程序的新接口设置对话框，选中能够与位于另外一个子网中的 DHCP 服务器直接通信的那个接口选项（通常该接口就是连接另外一个子网的网卡）。选好目标接口之后，单击“确定”按钮，弹出如图 12-46 所示的“DHCP 中继站属性”

设置对话框。



图 12-45 选择“新增接口”命令

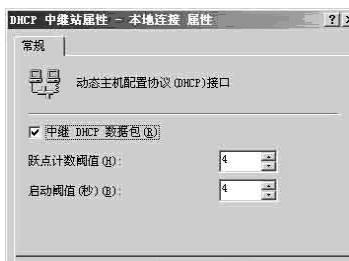


图 12-46 “DHCP 中继站属性”设置对话框

c. 将图 12-46 中的“中继 DHCP 数据报”复选框选中，同时设置好“跃点计数阈值”，以及“启动阈值”这两个参数（一般保持默认数值），最后单击“确定”按钮，这样 DHCP 中继代理功能就开始发挥作用了。

至此，DHCP 中继代理程序就能实现跨子网地址申请中转服务了；以后，与 DHCP 中继代理服务器位于相同子网的工作站，就能通过 DHCP 中继代理程序来向位于另外一个子网的 DHCP 服务器申请动态 IP 地址了。

3. Linux 下 DHCP 配置

在 Linux 下配置 DHCP，主要的工作是对相关文件进行解析。

(1) DHCP 启动与停止

可以使用以下命令来启动、停止和重启 dhcpd 服务器程序：

```
[root@lib1 root] # service dhcpd [ start | stop | restart ]
```

或

```
[root@lib1 root] # /etc/init.d/dhcpd [ start | stop | restart ]
```

其中 start、stop、restart 为任选参数，分别表示启动、停止和重启。执行以上命令启动后，dhcpd 默认是启动在 eth0 上的，如果 dhcpd 上的服务器还有另外一块网卡 eth1，想在 eth1 上启动 dhcpd，就输入：

```
[root@lib1 root] # /usr/sbin/dhcpd eth1
```

(2) 配置文件解析

DHCP 默认的配置文件是/etc/dhcpd.conf，它是一个递归下降格式的配置文件，有点像 C 语言的源程序风格，由参数和声明两大类语句构成，参数类语句主要告诉 DHCPd 网络参数，如租约时间、网关、DNS 等；而声明语句则用来描述网络的拓扑，表明网络上的客户，要提供给客户的 IP 地址，提供一个参数组给一组声明等。参数类又分为标准参数语句和选项类语句，这里给出 dhcpd.conf 配置文件中最常用和最重要的语句。

① 参数类与选项类语句

DHCP 配置语句如表 12-6 所示。

表 12-6 DHCP 配置语句

类型	语 句 格 式	功能与参数描述
标准参数类语句	ddns-update-style type	动态 DNS 解析方式，可选参数分别为：ad-hoc、interim、none
	default-lease-time time	指定默认租约时间，这里的 time 是以秒为单位的。如果 DHCP 客户在请求一个租约时没有指定租约的失效时间，租约时间就是默认租约时间
	max-lease-time time	最大的租约时间。如果 DHCP 在请求租约时间时发出特定的租约失效时间的请求，则用最大租约时间
	Hardware hardware-type hardware-address	指明物理硬件接口类型和硬件地址。硬件地址由 6 个 8 位组构成，每个 8 位组以 “:” 隔开。如 00:00:E8:1B:54:97
	server-name “name”	用于告知客户端所连接服务器的名字
	fixed-address address [, address ...]	用于指定一个或多个 IP 地址给一个 DHCP 客户，只能出现在 host 声明里
选项类语句	option subnet-mask mask	DHCP 服务配置子网掩码选项，服务开启后可应用于所有客户端
	option broadcast-address IP 地址	DHCP 服务配置广播地址选项，服务开启后可应用于所有客户端
	option routers IP 地址	同上，DHCP 服务配置网关（路由）地址选项，可设多个
	option domain-name-servers IP 地址	DHCP 服务配置 DNS 服务器地址，可应用于所有客户端，可设多个
	option domain-name “csai.cn”	DHCP 服务配置域名服务，可应用于所有客户端
	option host-name string	给客户指定主机名，string 是一个字符串

② 声明类语句

• share-network 语句

```
shared-network name {
[ 参数 ]
[ 声明 ]
}
```

share-network 用于告诉 DHCP 服务器某些 IP 子网其实是共享同一个物理网络的。任何一个在共享物理网络里的子网都必须在 share-network 语句中声明。当属于其子网里的客户启动时，将获得在 share-network 语句中指定的参数，除非这些参数被 subnet 或 host 里的参数覆盖。使用 share-network 是一种权宜之计，例如，某公司用 B 类网络 145.252.0.0，公司里的部门 A 被划在子网 145.252.1.0 里，子网掩码为 255.255.255.0，这里子网号为 8 位，主机号也为 8 位，但如果部门 A 急速增长，超过了 254 个节点，而物理网络还来不及增加，就要在原来这个物理网络上跑两个 8 位掩码的子网，而这两个子网其实是在同一个物理网络上的。share-network 语句如下：

```
shared-network share1 {                                # share1 这里是共享网络名
subnet 145.252.1.0 netmask 255.255.255.0 {
range 145.252.1.10 145.252.1.253;
}
subnet 145.252.2.0 netmask 255.255.255.0 {
range 145.252.2.10 145.252.1.253;
}
}
subnet 语句
subnet subnet-number netmask netmask {
[ 参数 ]
[ 声明 ]
}
```

subnet 语句用于提供足够的信息来阐明一个 IP 地址是否属于该子网。也可以提供指定

的子网参数和指明哪些属于该子网的 IP 地址可以动态分配给客户, 这些 IP 地址必须在 `range` 声明里指定。`subnet-number` 可以是 IP 地址或能被解析到这个子网的子网号的域名。`netmask` 可以是 IP 地址或能被解析到这个子网的掩码的域名。例如:

```
subnet 192.168.0.1 netmask 255.255.255.0 {      # 子网声明和掩码
range 192.168.1.10 192.168.1.100;              # 地址段范围
range 192.168.1.150 192.168.1.200;            # 地址段范围
}
```

这段配置代码将允许 DHCP 服务器分配两段地址范围给 DHCP 客户机, 192.168.1.10~192.168.1.100 和 192.168.1.150~192.168.1.200。服务器发送下面的参数给 DHCP 客户机: 子网掩码是 255.255.255.0, 广播地址是 192.168.1.255, 默认网关是 192.168.1.1, DNS 是 192.168.1.1。

- **range 语句**

```
range [ dynamic-bootp ] low-address [ high-address];
```

在任何一个有动态分配 IP 地址的 `subnet` 语句中, 至少要有一个 `range` 语句, 用来指明要分配的 IP 地址的范围。如果只指定一个要分配的 IP 地址, 高地址部分可以省略。

- **host 语句**

`host` 语句的作用是为特定的客户机提供网络信息。

```
host hostname {
[ 参数 ]
[ 声明 ]
}
```

例如, 如果为一台名为 `WebServer` 的主机指定固定的 IP 地址, 则可以在 `dhcpd.conf` 文件中添加如下语句:

```
host WebServer {
hardware ethernet 08:00:00:4c:58:23;    # 指定主机上网卡接口及硬件地址
fixed-address 192.168.1.210;            # 固定 IP, 这两条命令参见参数类语句
}
```

- **group 语句**

`group` 语句给一组声明提供参数。

```
group {
[ 参数 ]
[ 声明 ]
}
```

- **allow 和 deny 语句**

`allow` 和 `deny` 语句用来控制 DHCPd 对客户的请求。它们有两个可选关键字, 即: `unknown-clients` 关键字和 `bootp` 关键字。

```
allow [ unknown-clients | bootp ];
deny  [ unknown-clients | bootp ];
```

`allow unknown-clients` 允许 DHCPd 可以动态分配 IP 地址给未知的客户机, 而 `deny unknown-clients` 则不允许, 默认是允许的。`bootp` 关键字指明 DHCPd 是否响应 `bootp` 查询, 默认是允许的。

(3) dhcpd.leases 文件解析

dhcpd.leases 是 DHCP 客户租约的数据库文件，默认目录为/var/state/dhcp/，文件包含租约声明，每次一个租约被获取、更新或释放时，它的新值就被记录到文件的末尾。

```
Lease ip-address { statements... }
```

每个记录包含一个提供给客户的 IP 地址，在大括号里“{ }”的语句包含一些租约信息。具体的租约信息因客户发出不同的 DHCP 请求而稍有差别。

例如，在主机 CSAI_USER 获得租约后，dhcpd 会在 dhcp.leases 里建一条记录：

```
lease 192.168.1.100 {  
starts 1 2000/05/15 13:36:42 ;  
ends 1 2000/05/15 21:36:42 ;  
hardware ethernet 00:00:21:4e:3f:58 ;  
uid 01:00:00:21:4e:3f:58 ;  
client-hostname "CSAI_USER" ;  
}
```

要注意的是，dhcpd.leases 的时间记录采用 GMT 时间，而不是本地时区的时间 (GMT+8:00)。

以上就是 DHCPd 常用配置，在实际应用 DHCP 时还要考虑 IP 分配的一些策略问题，同时要保证网络的健壮性，必须至少要有两台 DHCP 服务器一起工作，如果一台出了故障，另一台可以继续为 DHCP 客户服务。然而，目前 DHCP 协议里并没有能让两台 DHCP 服务器协同工作的机制，不能保证分配的地址的唯一性，所以这两台 DHCP 服务器里的可分配地址空间必须进行调整，不能有交叉重复的 IP 地址。

12.4.2 一点一练

试题 1

DHCP 客户端启动时会向网络发出一个 Dhcpdiscover 包来请求 IP 地址，其源 IP 地址为____(1)_____。

- (1) A. 192.168.0.1 B. 0.0.0.0
C. 255.255.255.0 D. 255.255.255.255

试题 2

当使用时间到达租约期的____(2)_____时，DHCP 客户端和 DHCP 服务器将更新租约。

- (2) A. 50% B. 75% C. 87.5% D. 100%

试题 3

Linux 系统中，默认安装 DHCP 服务的配置文件为____(3)_____。

- (3) A. /etc/dhcpd.conf B. /etc/dhcp.conf
C. /etc/dhcpd.config D. /etc/dhcp.config

试题 4

以下关于 DHCP 协议的描述中，错误的是____(4)_____。

- (4) A. DHCP 客户机可以从外网段获取 IP 地址
B. DHCP 客户机只能收到一个 dhcpoffer
C. DHCP 不会同时租借相同的 IP 地址给两台主机
D. DHCP 分配的 IP 地址默认租约期为 8 天

试题 5

在 Windows 系统中需要重新从 DHCP 服务器获取 IP 地址时，可以使用____(5)_____命令。

(5) A. `ipconfig -a` B. `ipconfig` C. `ipconfig/all` D. `ipconfig/renew`

12.4.3 解析与答案

试题 1 分析

DHCP 是基于客户机-服务器模型设计的, DHCP 客户机和 DHCP 服务器之间通过收发 DHCP 消息进行通信, 如图 12-47 所示。

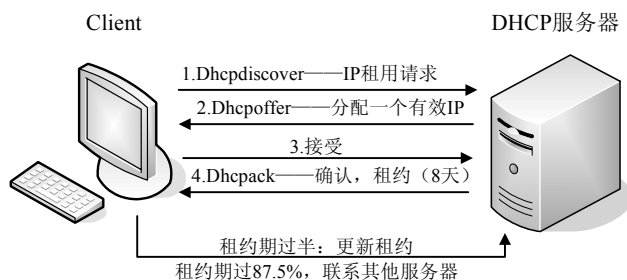


图 12-47 DHCP 服务过程

不论是 DHCP 客户机还是 DHCP 服务器, 都是通过按 DHCP 消息格式要求来填写各个段的, 形成具体的 DHCP 消息, DHCP 使用的传输协议是非面向连接的 UDP (用户数据报协议), 从 DHCP 客户机发出的 DHCP 消息送往 DHCP 服务器的端口 67, DHCP 服务器发给客户的 DHCP 消息送往 DHCP 客户的端口 68, 由于在取得服务器赋予的 IP 之前, DHCP 客户并没有自己的 IP, 所以包含 DHCP 消息的 UDP 数据报的 IP 头的源地址段是 0.0.0.0, 目的地址则是 255.255.255.255。

试题 1 答案

(1) B

试题 2 分析

关于 IP 地址租约的问题, 需要注意的是, 当 DHCP 客户机租期达 50%时, 重新更新租约, 客户机发送 `DHCPRequest` 包。当租约达到 87.5%时, 进入重新申请状态, 客户机发送 `DHCPDiscover` 包。

试题 2 答案

(2) A

试题 3 分析

本题考查 Linux 系统下 DHCP 服务的配置文件存放位置。

试题 3 答案

(3) A

试题 4 分析

本题考查考生对 DHCP 协议的掌握程度。

借助中继代理, DHCP 客户机可以从外网段获取 IP 地址; DHCP 不会同时租借相同的 IP 地址给两台主机; 默认情况下, DHCP 分配的 IP 地址租约期为 8 天; DHCP 客户机可以收到多个 `dhcpoffer`, 通常从中选择最先到达的作为本机的 IP 地址。

试题 4 答案

(4) B

试题 5 分析

本试题考查考生对 `ipconfig` 命令的运用。

`ipconfig` 是最常用的 Windows 实用程序，可以显示所有网卡的 TCP/IP 配置参数，刷新动态主机配置协议（DHCP）和域名系统（DNS）的设置。

`ipconfig/all` 用于显示所有网卡的 TCP/IP 配置信息。如果没有该参数，则只显示各个网卡的 IP 地址、子网掩码和默认网关地址。

`ipconfig /renew` 用于更新网卡的 DHCP 配置，如果使用标识符 `Adapter` 说明了网卡的名字，则只更新指定网卡的配置，否则就更新所有网卡的配置。

试题 5 答案

(5) D

12.5 Samba 和 Apache 服务器

在 Samba 和 Apache 服务器这个考点中，主要涉及两个方面的知识，分别是 Linux 系统下 Samba 服务器配置和 Linux 系统下 Apache 服务器配置。

12.5.1 考点精讲

Samba (smb) 是为 Linux-Windows 互联共享资源而设计的程序，主要用于不同操作平台间文件和打印机共享。它也一样用于 Linux 和 Linux 之间的文件共享；不过，对于 Linux 和 Linux 之间共享文件有更好的网络文件系统 NFS。Samba 有两个服务程序，即 `smb` 和 `nmb`，`smb` 是 Samba 的主要启动服务，让其他机器能知道此机器共享了什么；`nmb` 是把这台 Linux 机器所共享的工作组及在此工作组下的 NetBIOS Name 解析出来，如果不打开 `nmb` 服务器，只能通过 IP 来访问。

Apache 是世界使用量排名第一的 Web 服务器软件。它可以运行在几乎所有广泛使用的计算机平台上，由于其跨平台和安全性被广泛使用，目前它是世界上最流行的 Web 服务器端软件之一。

1. Samba 服务器配置

(1) Samba 基础配置

① Samba 启动

用以下命令可以直接启动、关闭与重启 Samba 服务：

```
[root@lib1 root] # service smb [ start | stop | restart ]
```

或

```
[root@lib1 root] # etc/init.d/smb [ start | stop | restart ]
```

其中 `start`、`stop`、`restart` 为任选参数，分别表示启动、停止和重启。

② smb.conf

Samba 服务的配置文件是 `etc/init.d/smb.conf`。此文件中用“#”和“;”表示注释语句。`smb.conf` 文件有以下 3 个主要部分。

- 全局参数字段（`global`）：主机共享时的整体设置。
- 目录共享字段（`homes`）：定义一般参数，如建立共享文件目录等。
- 打印机共享字段（`printers`）：打印机的配置和共享。

下面对 `smb.conf` 文件中的主要设置项进行逐一解释说明。

- `[global]`


```
workgroup = CSAIGROUP
# 此参数设置服务器所要加入工作组的名称，系统默认为 MYGROUP。
netbios name = LinuxSir
# 此参数在配置文件中未列出，需要手动添加，用于设置显示在“网上邻居”中的主机名。
server string = Linux Samba
# 此参数描述 Samba 服务器的一些信息，这些注释信息会显示在“网上邻居”中。
security = [ user | share | Server | Domain ]
# 此可选参数用于设置 Samba 服务器的安全模式。
```

user 模式：当主机访问 Samba 服务器时，需要输入用户名与密码，该用户必须属于服务器注册用户。

share 模式：当主机访问 Samba 服务器时，不需要输入用户名与密码，即对所有主机或用户共享。

Server 模式：需要输入用户名与密码，验证用户信息由另一个服务器负责，而非 Samba 服务器。

Domain 模式：与 Server 模式类似，使用域中的服务器来验证用户信息。

```
Host allow = 192.168.1 192.168.2. 127.
#此参数设置哪些 IP 允许访问该服务器，本例中允许的网段分别是 192.168.1.0、192.168.2.0
和 127.0.0.0。
dns proxy = [ yes | no ]      # 此参数设置 Samba 服务器是否作为 DNS 服务的代理解析。
```

• [homes]

```
comment = Home Directories      # 对共享资源的注释说明。
path = /home/share              # 设置共享目录的路径。
browseable = [ yes | no ]       # 设置是否允许浏览文件或目录。
writable = [ yes | no ]         # 设置是否允许往目录里写入文件。
Valid users = %S|%cs
# 设置可访问的用户，系统会自动将%S转换成登录账号。@cs 表示 cs 用户组下的所有用户可以访问
samba 服务器。
create mask = 0664
#create mask 是用户创建文件时的权限掩码，对用户可读/可写，对用户组可读/可写，对其他用
户可读。
directory mask = 0775
#directory mask 用来设置用户创建目录时的权限掩码，意思是对于用户和用户组可读/可写，对
其他用户可读/可执行。
```

• [printers]

```
comment = all printers
path = /var/spool/samba          # 设置打印机队列位置。
browseable = [ yes | no ]       # 设置是否允许浏览打印机。
Guest ok = [ yes | no ]         # 访问打印机时是否需要密码。
writable = [ yes | no ]         # 共享打印机必须设置为 NO。
```

(2) Samba 用户管理

① 导入系统用户

Samba 服务的用户必须保证是 Linux 系统已存在的用户，因此在添加 Samba 用户前，可以使用如下命令将系统用户导入到 Samba 服务中：

```
[root@lib1 samba] # cat /ect/passwd | mksmbpasswd.sh > /ect/samba/smbpasswd
```

② 添加新用户

可以为 Samba 服务添加单个新用户，添加的新用户必须是已存在的系统用户。先按照

下面命令建立系统用户：

```
[root@lib1 samba] # useradd csaiuser1
```

再将其添加到 Samba 服务用户中：

```
[root@lib1 samba] # sambadduser csaiuser1: csaiuser1
```

(3) Samba 共享配置

下面给出一个具体实例：假设在服务器上设置一个共享目录 **public**，不需要用户名与密码就可以为所有用户共享访问，并为用户 **csaiuser1** 创建个人目录 **/usr/csaiuser1_dir**，只有 **csaiuser1** 可以访问。

① 创建目录及共享资源并设置权限

在 **/home** 目录下创建 **public** 目录，设置权限为可读/写。在 **/usr** 目录下创建 **csaiuser1_dir** 目录，设置权限为可读/写。

```
[root@lib1 home] # mkdir public
[root@lib1 home] # chmod 777 public
[root@lib1 usr] # mkdir csaiuser1_dir
[root@lib1 home] # chmod 777 csaiuser1_dir
```

② 修改 smb.conf 文件

在 **share definitions** 区域添加如下内容：

```
[public]
comment = public directories
browseable = yes
path = /home/public
writable = yes
public = yes
[csaiuser1_dir]
comment = user1 directories
path = /usr/ csaiuser1_dir
valid users = csaiuser1
writable = yes
public = no
```

文修改件后，必须重启 Samba 服务器才能生效。

(4) Linux 访问 Windows

Linux 主机访问 Windows 主机资源时，可以使用两个命令：**smbclient** 或 **smbmount**。下面分别以 Linux 主机 Lib1 (192.168.0.1) 配置为 Samba 服务器，访问 Windows 主机 Lib2 (192.168.0.2) 上的共享资源 **D:/Win_share** 目录为例进行介绍。

① smbclient 命令

该命令既可以查看并访问 Windows 主机提供的共享资源，也可以查看本机（Samba 服务器）提供的共享资源。

- 查看本机提供的资源时，命令如下：

```
[root@lib1 samba] # smbclient -L Localhost
```

- 查看 Windows 主机提供的资源时，命令如下：

```
[root@lib1 samba] # smbclient -L lib2 -U administrator
```

- 查看 Windows 主机提供的资源时，命令如下：

```
[root@lib1 samba] # smbclient //lib2/win_share -U administrator
smb:\>
```

在 `smb:\>` 提示符后，可以使用如 FTP 一样的命令方法来使用 `smbclient`。如 `dir:` 显示当前共享目录信息；`get:` 下载所需要的文件。

② smbmount 命令

该命令可将共享的 Windows 目录直接挂载到 Linux 系统的本地目录（类似于磁盘映射）。这样可以像访问本机目录一样来操作挂载目录，从而访问 Windows 主机资源。

```
[root@lib1 samba] # mkdir /mnt/samba
[root@lib1 samba] # smbmount //lib2/win_share /mnt/samba username = csaiuser1
```

卸载已挂载目录中已使用 `umount` 命令：

```
[root@lib1 samba] # umount /mnt/samba
```

③ Windows 访问 Linux

打开 Windows 的 IE 浏览器，用 IP 地址的访问方式就可以访问了，格式为 `\\192.168.0.1`。也可以通过网上邻居等传统 Windows 访问方式访问 Linux 资源。

2. Apache 服务器配置

(1) Apache 基础配置

可以设置每次启动计算机时，`httpd` 自动开启。也可以使用下面的命令手动开启或关闭它（以 `root` 权限）：`/etc/rc.d/init.d/httpd [start|stop]`

① 全局配置项

`httpd.conf` 是 Apache 服务器的配置文件，其绝对路径为 `/etc/httpd/conf/httpd.conf`。此文件中包括相当数量的全局配置项，这些配置项不包含在任何区域中，它们决定了 Apache 服务器的全局参数。在此配置文件中常见的全局配置项及其含义如下。

- **ServerRoot:** 用于设置 `httpd` 服务器的根目录，该目录中包括了运行 Web 站点必须的目录和文件。默认的根目录为 `“/etc/httpd/”`，在 `httpd.conf` 配置文件中，如果设置的目录或文件不是用绝对路径，都认为是在服务器根目录下。
- **Listen:** 用于设置 Apache 服务器监听的网络端口号，默认为 80。
- **User:** 用于设置运行 `httpd` 进程时的用户身份，系统默认为 `daemon` 用户。
- **Group:** 用于设置运行 `httpd` 进程时的组身份，系统默认为 `daemon` 组。
- **Server Admin:** 用来设置 Web 管理员的 E-mail 地址。这个地址会出现在系统连接出错的时候，以便访问者能够将情况及时地告知 Web 管理员。
- **ServerName:** 用来配置网站服务器的域名。
- **DocumentRoot:** 用于设置网页文档根目录在系统中的实际路径。`DocumentRoot` 配置项比较容易与 `ServerRoot` 混淆，需要格外注意。
- **DirectoryIndex:** 用于声明首页文件名称。一般使用 `index.html` 或 `index.htm` 作为首页的文件名。如果这样设置后，那么客户端发出 Web 服务请求时，首先调入的主页是在指定目录下的 `index.html` 或 `index.htm`。
- **ErrorLog:** 用于指定错误日志文件名称和路径。
- **LogLevel:** 用于设置记录日志的级别，默认为 `Warn`（警告）。
- **CustomLog:** 用于设置 Apache 服务器中访问日志文件的路径和格式类型。

- **PidFile**: 用于设置保存 httpd 服务器程序进程号 (PID) 的文件, 默认设置为 “logs/httpd.pid”, “logs” 目录位于 Apache 服务器根目录中。
- **Timeout** 命令: 用于设置 Web 服务器与浏览器之间网络连接的超时秒数, 默认为 300 秒。
- **KeepAlive**: 用于设置是否使用保持连接功能。设置为 Off 时表示不使用, 客户机的每次连接只能从服务器请求返回一个文件, 传输的效率比较低; 当设置为 On 时, 客户机与服务器建立一次连接后可以请求传输多个文件, 将提高服务器传输文件的效率。
- **MaxKeepAliveRequests**: 用于设置客户端每次连接允许请求响应的最大文件数, 默认设置为 100 个。当 KeepAlive 设置为 On 时才生效。
- **MaxKeepAliveTimeout**: 用于设置保持连接的超时秒数, 当客户机的两次相邻连接请求超过该设置值时需要重新进行连接请求, 默认设置值为 15 秒。
- **Include**: 用户包含另一个配置文件的内容, 可以将一些特殊功能的配置单独放到一个文件中, 再使用 Include 配置项包含到 httpd.conf 主配置文件中来, 便于独立维护。

以上配置项是 httpd.conf 文件中最主要的全局配置项, 还有很多其他配置项, 这里不再一一列举。

② 区域设置

在 httpd.conf 中除了有全局配置项外, 大多数配置都是包含在区域中的。区域设置使用一对组合标记, 限定了配置项的作用范围。常见的目录区域格式如下:

```
<Directory /home/httpd/html>
Option Indexes Includes ExecCGI FollowSymLink
AllowOverride None
Order allow , deny
allow from all
</Directory>
```

这部分是以 “<Directory /home/httpd/html>” 开始, 以 “</Directory>” 结束的, 其中间的部分都是针对指定目录 “/home/httpd/html” 而言的。相关选项说明如下。

- **Option** 命令有很多的参数, 各个参数表示允许某项功能, 如 All 表示允许所有功能。
- **AllowOverride** 命令则用来决定是否允许在 “httpd.conf” 文件中设定权限, 是否可以被文件 “.htaccess” 中设定的权限覆盖。它有两个参数: All 表示允许覆盖; None 表示不允许覆盖。
- **Order** 命令用来设定谁能从这个服务器上取得控制。它也有两个参数: allow 表示可以取得控制; deny 表示禁止取得控制。

目录 “/home/httpd/html” 的设置含义是: 它使得这个目录在不存在 index.htm 文件时, 列出目录信息以供选择, 允许 SSI, 允许执行 CGI 程序, 开启了动态连接。

在上面代码中, 有可能已经根据新的需求更改了相应的配置选项, 如果要使这个新的配置立即生效, 就必须重新启动 Web 服务进程。在 Linux 中, 可以十分方便地使用命令行来使得 Web 服务进程重启: /etc/rc.d/init.d/httpd restart。

(2) 个人主页空间

如果利用 Linux 系统架设了一台 Web 服务器, 那么我们不仅可以存放公司的主页, 而且还可以为公司的每一个员工提供一块个人主页的空间。

首先，在 Linux 上为需要个人主页空间的用户开设一个账号。这样，他就拥有了一个用户主目录“/home/用户账号名”。执行命令：

```
addusr 用户账号名          # 添加用户账号并设置登录密码
passwd 用户密码            # 为用户设定登录口令
```

然后，在用户主目录下建立一个目录 `public_html`，为其设置相应的权限，执行命令：

```
cd 用户账号名              # 进入到用户宿主目录
mkdir public_html          # 创建个人主页目录并设置目录权限为 755
chmod 755 public_html      # 更改权限
```

接着利用 `UserDir` 命令，用来指定个人主页的位置。如果有一个用户 `test`，它的主目录是“/home/test”，当客户端输入 `http://www.csai.cn/~test` 时，系统就会到对应的目录“/home/test/UserDir/”中去寻找。其中，`UserDir` 是在 `httpd.conf` 配置文件中用 `UserDir` 命令设置的指定目录。命令格式如下：

```
UserDir [Path]             #指定用户宿主目录下的网页根目录
```

例如：`UserDir public_html`

最后，确认在 `httpd.conf` 文件中的 `UserDir` 命令设置的是 `public_html` 目录。让员工将自己的个人主页上传到自己用户主目录下的 `public_html` 目录中。现在就可以使用“`http://www.csai.cn/~用户账号名`”来访问员工的个人主页了。

（3）虚拟主机服务

所谓的虚拟主机服务就是指将一台机器虚拟成多台 Web 服务器。虚拟服务器选用一台功能较强大的大型服务器，然后用虚拟主机的形式，提供多个企业的 Web 服务，虽然所有的 Web 服务都是由这台服务器提供的，但是让访问者看起来却与在不同的服务器上获得 Web 服务一样。用 Apache 设置虚拟主机服务通常可以采用两种方案：基于 IP 地址的虚拟主机和基于名字的虚拟主机。

① 基于 IP 地址的虚拟主机服务

这种方式需要在机器上设置 IP 别名，也就是在一台机器的网卡上绑定多个 IP 地址去为多个虚拟主机服务。假设，我们用来实现虚拟主机服务的机器，首先已经为自己提供了 Web 服务，现在将为新的一家 `www.csai.cn` 提供虚拟主机服务。配置步骤如下。

- 规划 IP 地址：为虚拟主机申请新的 IP 地址（假设本机 IP 地址为 202.101.2.1）。

```
www.csai.cn 202.101.2.2
```

- 让 ISP 做好相应的域名解析工作。

- 为网卡设置 IP 别名：

```
/sbin/ifconfig eth0:0 202.101.2.2 netmask 255.255.255.0
```

- 重新设置“/etc/httpd/conf/httpd.conf”，在文件中加入：

```
<VirtualHost 202.101.2.2>
    ServerAdmin webmaster@csai.cn
    DocumentRoot /home/httpd/www.csai.cn
    ServerName www.csai.cn
    ErrorLog /var/log/httpd/www.csai.cn/error.log
</VirtualHost>
```

- 建立相应的目录：

```
mkdir /home/httpd/www.csai.cn
```

```
mkdir /var/log/httpd/www.csai.cn/error.log
```

- 将相应的主页内容存放在相应的目录中即可。

② 基于名字的虚拟主机服务

配置基于名字的虚拟主机服务需要修改配置文件“/etc/httpd/conf/httpd.conf”，在这个配置文件中增加以下内容：

```
NameVirtualHost 202.101.2.1
<VirtualHost 202.101.2.1>
ServerAdmin webmaster@csai.cn
    DocumentRoot /home/httpd/www.csai.cn
    ServerName www.csai.cn
    ErrorLog /var/log/httpd/www.csai.cn/error.log
</VirtualHost>
<VirtualHost 202.101.2.1>
ServerAdmin webmaster@educity.cn
    DocumentRoot /home/httpd/www.educity.cn
    ServerName www.educity.cn
    ErrorLog /var/log/httpd/www.educity.cn/error.log
</VirtualHost>
```

也就是在基于 IP 地址的配置基础上增加一句“NameVirtualHost 202.101.2.1”而已。在本例中，为了体现只需要增加一次，所以特别地设置了两个虚拟主机服务。最后也是建立相应的目录，将主页内容放到相应的目录中去就可以了。

12.5.2 一点一练

试题 1

Linux 系统中， (1) 服务的作用与 Windows 的共享文件服务作用相似，提供基于网络的共享文件/打印服务。

- (1) A. Samba B. Ftp C. SMTP D. Telnet

试题 2

在一台 Apache 服务器上通过虚拟主机可以实现多个 Web 站点。虚拟主机可以是基于 (2) 的虚拟主机，也可以是基于名字的虚拟主机。

- (2) A. IP B. TCP C. UDP D. HTTP

试题 3

若某公司创建名字为 www.business.com 的虚拟主机，则需要 (3) 服务器中添加地址记录。

- (3) A. SNMP B. DNS C. SMTP D. FTP

试题 4

在 Linux 中该地址记录的配置信息如下，请补充完整。

```
NameVirtualHost 192.168.0.1
<VirtualHost 192.168.0.1>
    (4) www.business.com
    DocumentRoot /var/www/html/business
</VirtualHost>
```

- (4) A. WebName B. HostName C. ServerName D. WWW

试题 5

为保障 Web 服务器的安全运行，对用户要进行身份验证。关于 Windows Server 2003 中

的“集成 Windows 身份验证”，下列说法中错误的是____(5)____。

- (5) A. 在这种身份验证方式中，用户名和密码在发送前要经过加密处理，所以是一种安全的身份验证方案
- B. 这种身份验证方案结合了 Windows NT 质询/响应身份验证和 Kerberos v5 身份验证两种方式
- C. 如果用户系统在域控制器中安装了活动目录服务，而且浏览器支持 Kerberos v5 身份认证协议，则使用 Kerberos v5 身份验证
- D. 客户机通过代理服务器建立连接时，可采用集成 Windows 身份验证方案进行验证

12.5.3 解析与答案

试题 1 分析

本题考查在 Linux 系统中 Samba 服务的基本概念。

试题 1 答案

(1) A

试题 2 分析

Apache 服务器可以实现基于 IP 和基于名字的虚拟主机。基于 IP 的虚拟主机方式需要在机器上设置 IP 别名，如在一台机器的网卡上绑定多个 IP 地址去服务多个虚拟主机。这种基于 IP 的虚拟主机有一个缺点，就是你需要更多的 IP 地址去服务各自的虚拟主机，若 IP 地址不够，则不可采用此方式。基于名字的虚拟主机只需要在 Apache 的配置文件中，对 NameVirtualHost 域中 DocumentRoot 和 ServerName 分别设定其对应的虚拟主机的文档路径即可。

试题 2 答案

(2) A

试题 3 分析

为了使不同的名字指向同一个 IP 地址，基于名字的虚拟主机还必须修改 DNS 服务器上的 A 记录，让不同名字的域都指向同一个服务器 IP 地址。

试题 3 答案

(3) B

试题 4 分析

基于名字的虚拟主机只需要在 Apache 的配置文件中，对 NameVirtualHost 域中 DocumentRoot 和 ServerName 分别设定其对应的虚拟主机的文档路径即可。

试题 4 答案

(4) C

试题 5 分析

在集成 Windows 身份验证方式中，用户名和密码在发送前要经过加密处理，所以是一种安全的身份验证方案。这种身份验证方案结合了 Windows NT 质询/响应身份验证 (NTLM) 和 Kerberos v5 身份验证两种方式。Kerberos v5 是 Windows 2000 分布式服务架构的重要功能，为了进行 Kerberos v5 身份验证，客户机和服务器都必须与密钥发行中心 (KDC) 建立可信任的连接。如果用户系统在域控制器中安装了 Active Directory 服务，而且浏览器支持 Kerberos v5 身份认证协议，则使用 Kerberos v5 身份验证，否则使用 NTLM 身份验证。

集成 Windows 身份验证的过程如下。

① 在这种认证方式下,用户不必输入凭据,而是使用客户机上当前的 Windows 用户信息作为输入的凭据。

② 如果最初的信息交换未能识别用户的合法身份,则浏览器将提示用户输入账号和密码,直到用户输入了有效的账号和密码,或者关闭了提示对话框。

集成 Windows 身份验证方案虽然比较安全,但是通过代理服务器建立连接时这个方案就行不通了。所以集成 Windows 身份验证最适合于 Intranet 环境,这样用户和 Web 服务器都在同一个域内,而且管理员可以保证每个用户浏览器都在 IE 2.0 版本以上,保证支持这种身份验证方案。

试题 5 答案

(5) D

12.6 代理服务

在代理服务这个考点中,主要涉及两个方面的知识,分别是代理服务器的原理和功能、Linux 系统下 squid 代理服务器配置。

12.6.1 考点精讲

代理服务器英文全称是 Proxy Server,其功能就是代理网络用户去取得网络信息。形象地说:它是网络信息的中转站。在一般情况下,我们使用网络浏览器直接去连接其他 Internet 站点取得网络信息时,必须送出 Request 信号来得到回答,然后对方再把信息以 bit 方式传送回来。

Squid cache (简称为 Squid) 是一个流行的自由软件 (GNU 通用公共许可证) 的代理服务器和 Web 缓存服务器。Squid 有广泛的用途,可以作为网页服务器的前置 cache 服务器缓存相关请求来提高 Web 服务器的速度;可以为一组人共享网络资源而缓存万维网,域名系统和其他网络搜索;可以通过过滤流量帮助网络安全;还可以局域网通过代理上网。Squid 的发展历史相当悠久,功能也相当完善。除了 HTTP 外,对于 FTP 与 HTTPS 的支持也相当好。

1. 代理服务器工作原理

代理服务器是介于浏览器和服务器的另一台服务器,是网络信息的中转站。使用代理功能后,浏览器将首先向代理服务器发送请求,进而由代理服务器完成请求内容,将数据再返回给浏览器。代理服务器的工作流程如图 12-48 所示。

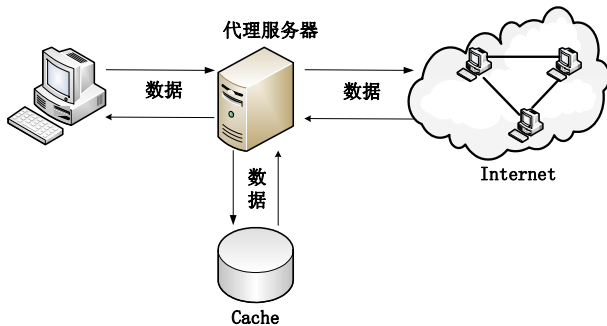


图 12-48 代理服务器的工作流程

2. 代理服务器功能

一般说来,代理服务器具有以下的功能。

(1) 通过缓存增加访问速度

通过代理服务器的缓存功能来加快网络的访问速度。一般说来,大多数的代理服务器都支持 HTTP 缓存,但是,有的代理服务器也支持 FTP 缓存。在选择代理服务器时,对于大多数的组织,只需要 HTTP 缓存功能就足够了。通常,缓存有被动缓存和主动缓存之分。

① 被动缓存:指的是代理服务器只在客户机请求数据时才将服务器返回的数据进行缓存,如果数据过期了,又有客户机请求相同数据时,代理服务器又必须重新发起新的数据请求,在将响应数据传送给客户端时又进行新的缓存。

② 主动缓存:就是代理服务器不断地检查缓存中的数据,一旦有数据过期,则代理服务器主动发起新的数据请求来更新数据。这样,当有客户机请求该数据时就会大大缩短响应时间。

(2) 提供私有 IP 访问 Internet 的方法

IP 地址是不可再生的宝贵资源,假如你只有有限的 IP 地址,但是需要提供整个组织的 Internet 访问能力,那么你可以通过使用代理服务器来实现这一点。

(3) 提高网络的安全性

如果内部用户访问 Internet 都是通过代理服务器,那么代理服务器就成为进入 Internet 的唯一通道;反过来说,代理服务器也是 Internet 访问内部网的唯一通道,如果没有反向代理,那么对于 Internet 上的主机来说,整个内部网只有代理服务器是可见的,从而大大增强了网络的安全性。

3. Linux 下 squid 代理服务器

下面介绍 squid.conf 文件的结构以及一些常用的选项。squid.conf 配置文件可以分为 13 个部分。如果只是为一个中小型网络提供代理服务,并且只准备使用一台服务器,那么配置问题将会变得相对简单,只需要修改配置文件中的几个选项即可满足应用需求。这几个常用选项分别介绍如下。

(1) http_port

该选项定义 Squid 监听 HTTPD 客户连接请求的端口,默认端口号是 3128,如果使用 HTTPD 加速模式,端口号则为 80。可以指定多个端口,但是所有指定的端口都必须在一行命令上出现,程序才能正确地识别。

(2) cache_mem (bytes)

该选项用于指定 Squid 可以使用的内存的理想值。这部分内存被用来存储以下对象: In-Transit objects(传入的对象)、Hot Objects(热对象,即用户常访问的对象)、Negative-Cached objects(消极存储的对象)。

(3) cache_dir Directory-Name Mbytes Level1 Level2

该选项指定 Squid 用来存储对象的交换空间的大小及其目录结构。可以用多个 cache_dir 命令来定义多个交换空间,并且这些交换空间可以分布在不同的磁盘分区。“Directory”指明了该交换空间的顶级目录。如果想用整个磁盘作为交换空间,那么可以将该目录作为挂载点将整个磁盘挂装上去。其默认值为/var/spool/squid。Mbytes 定义了可用的空间总量。

使用访问控制特性,可以控制在访问时根据特定的时间间隔进行缓存、访问特定站点或一组站点等。Squid 访问控制有两个要素:ACL 元素和访问列表。通过使用这些方法,系统管理员可以严格、清晰地定义代理服务器的访问控制策略。

(4) ACL 元素

该元素定义的语法如下：

```
acl aclname acltype stringl...  
acl aclname acltype "file"...
```

当使用文件时，该文件的格式为每行包含一个条目。其中，**acltype** 可以是任意一个在 ACL 中定义的名称；任何两个 ACL 元素不能用相同的名字；每个 ACL 由列表值组成，当进行匹配检测时，多个值由逻辑或运算连接。换句话说，任意一个 ACL 元素的值被匹配时，这个 ACL 元素即被匹配；并不是所有的 ACL 元素都能使用访问列表中的全部类型；不同的 ACL 元素写在不同行中，Squid 将这些元素组合在一个列表中。

(5) http_access 访问控制列表

根据访问控制列表允许或禁止某一类用户访问。如果某个访问没有相符合的项目，则默认为应用最后一条项目的“非”。比如最后一条为允许，则默认就是禁止。通常应该把最后的条目设为“deny all”或“allow all”来避免安全性隐患。下面给出使用这些访问控制方法的实例。

如果允许网段 10.0.0.124/24 以及 192.168.10.15/24 内的所有客户机访问代理服务器，并且允许在文件/etc/squid/guest 中列出的客户机访问代理服务器，除此之外的客户机将拒绝访问本地代理服务器。那么具体操作如下：

```
acl clients src 10.0.0.124/24 192.168.10.15/24  
acl guests src "/etc/squid/guest"  
acl all src 0.0.0.0/0.0.0.0  
http_access allow clients  
http_access allow guests  
http_access deny all
```

其中，文件“/etc/squid/guest”中的内容为：

```
172.168.10.3/24  
210.113.24.8/16  
10.0.1.24/25  
.....
```

如果允许域名为 csai.cn、educity.cn 的两个域访问本地代理服务器，其他的域都将拒绝访问本地代理服务器。那么具体操作如下：

```
acl permitted_domain src csai.cn educity.cn  
acl all src 0.0.0.0/0.0.0.0  
http_access allow permitted_domain  
http_access deny all
```

如果使用正则表达式，拒绝客户机通过代理服务器访问包含有诸如“sexy”等关键字的网站。那么具体操作如下：

```
acl deny_url url_regex - sexy  
http_access deny deny_url
```

如果拒绝客户机通过代理服务器访问文件中指定的 IP 或者域名的网站，其中文件/etc/squid/deny_ip 中存放有拒绝访问的 IP 地址，文件/etc/squid/deny_dns 中存放有拒绝访问的域名。那么具体操作如下：

```
acl deny_ip dst "/etc/squid/deny_ip"  
acl deny_dns dst "/etc/squid/deny_dns"  
http_access deny deny_ip
```

```
http_access deny deny_dns
```

如果允许和拒绝指定的用户访问指定的网站，比如允许客户 1 访问网站 <http://www.csai.cn>，而拒绝客户 2 访问网站 <http://www.educity.cn>。那么具体操作如下：

```
acl client1 src
acl client2 src
acl csai dst www.csai.cn
acl educity dst www.educity.cn
http access allow client1 csai
http access deny client2 educity
```

12.6.2 一点一练

试题 1

使用代理服务器（proxy server）访问 Internet 的主要功能不包括__（1）__。

- (1) A. 突破对某些网站的访问限制 B. 提高访问某些网站的速度
C. 避免来自 Internet 上的病毒的入侵 D. 隐藏本地主机的 IP 地址

试题 2

通过代理服务器使内部局域网中的客户机访问 Internet 时，__（2）__不属于代理服务器的功能。

- (2) A. 共享 IP 地址 B. 信息缓存
C. 信息转发 D. 信息加密

试题 3

使用代理服务器除了服务器端代理服务器软件需要配置外，客户端也需要配置使用代理服务器，且指向代理服务器的__（3）__。

- (3) A. MAC 地址和网络号 B. 邮件地址和网络号
C. IP 地址和网络号 D. IP 地址和端口号

试题 4

以下关于代理服务器功能描述最为正确的是__（4）__。

- (4) A. 提高客户端访问外网的效率 B. 隐藏企业内部网络细节
C. 节省 IP 开销 D. 以上答案都正确

试题 5

代理服务器实质上是一个架设在__（5）__用户群体与 Internet 之间的桥梁，用以实现用户对 Internet 的访问。

- (5) A. Internet B. 内部网络 C. 个人用户 D. 企业

12.6.3 解析与答案

试题 1 分析

代理服务器是介于浏览器和 Web 服务器之间的一台服务器，当用户通过代理服务器上网浏览时，浏览器不是直接到 Web 服务器去取回网页而是向代理服务器发出请求，由代理服务器来取回浏览器所需要的信息并传送到用户的浏览器。使用代理服务器访问 Internet 时可以突破对某些网站的访问限制、提高访问某些网站的速度、隐藏本地主机的 IP 地址，但是不能避免来自 Internet 上病毒的入侵。

试题 1 答案

- (1) C

试题 2 分析

代理服务器就是在计算机客户端和访问的计算机网络（通常是访问互联网）之间安装有相应代理服务器软件的一台计算机，客户端对网络的所有访问请求都通过代理服务器实现。而被访问的网络计算机对请求的回答，也通过代理服务器转达到客户端。

代理服务器的主要作用有以下四个。

- ① 代理服务器提供远程信息本地缓存功能，减少信息的重复传输。
- ② 所有使用代理服务器用户都必须通过代理服务器访问远程站点，因此在代理服务器上就可以设置相应的限制，以过滤或屏蔽掉某些信息。因此代理服务器可以起到防火墙的作用。
- ③ 通过代理服务器可访问一些不能直接访问的网站。互联网上有许多开放的代理服务器，客户在访问权限受到限制时，而这些代理服务器的访问权限是不受限制的，刚好代理服务器在客户的访问范围之内，那么客户通过代理服务器访问目标网络就成为可能。国内的高校多使用教育网，不能访问一些国外的互联网站点，但通过代理服务器，就能实现访问，这也是高校内流行使用代理服务器的原因所在。
- ④ 安全性得到提高。无论是上聊天室还是浏览网站。目的网站只能知道你来自于代理服务器，而你的真实 IP 无法测知，这就使得使用者的安全性得以提高。

试题 2 答案

(2) D

试题 3 分析

使用代理服务器除了服务器端代理服务器软件需要配置外，客户端也需要配置使用代理服务器，且指向代理服务器 IP 地址和端口号。

试题 3 答案

(3) D

试题 4 分析

代理服务器的主要功能如下。

- ① 设置用户验证和记账功能，可按用户进行记账，没有登记的用户无权通过代理服务器访问 Internet。并对用户的访问时间、访问地点、信息流量进行统计。
- ② 对用户进行分级管理，设置不同用户的访问权限，对外界或内部的 Internet 地址进行过滤，设置不同的访问权限。
- ③ 增加缓冲器（Cache），提高访问速度，对经常访问的地址创建缓冲区，大大提高热门站点的访问效率。通常代理服务器都设置一个较大的硬盘缓冲区（可能高达几个 GB 或更大），当有外界的信息通过时，同时也将其保存到缓冲区中，当其他用户再访问相同的信息时，则直接由缓冲区中取出信息，传给用户，以提高访问速度。
- ④ 连接内网与 Internet，充当防火墙（Firewall）：因为所有内部网的用户通过代理服务器访问外界时，只映射为一个 IP 地址，所以外界不能直接访问到内部网；同时可以设置 IP 地址过滤，限制内部网对外部的访问权限。
- ⑤ 节省 IP 开销：代理服务器允许使用大量的伪 IP 地址，节约网上资源，即用代理服务器可以减少对 IP 地址的需求，对于使用局域网方式接入 Internet，如果为局域网（LAN）内的每一个用户都申请一个 IP 地址，其费用可想而知。但使用代理服务器后，只需代理服务器上有一个合法的 IP 地址，LAN 内其他用户可以使用 10.×.×.× 这样的私有 IP 地址，这样可以节约大量的 IP，降低网络的维护成本。

试题 4 答案

(4) D

试题 5 分析

代理服务器就是在计算机客户端（通常是企业内部网络）和访问的计算机网络（通常是访问互联网）之间安装有相应代理服务器软件的一台计算机。客户端对网络的所有访问请求都通过代理服务器实现。而被访问的网络计算机对请求的回答，也通过代理服务器转达到客户端。

试题 5 答案

(5) B

12.7 考前冲刺

试题 1

若 DNS 资源记录中记录类型 (record-type) 为 A, 则记录的值为____(1)____。

(1) A. 名字服务器式 B. 主机描述 C. IP 地址 D. 别名

试题 2

在进行域名解析过程中, 由____(2)____获取的解析结果耗时最短。

(2) A. 主域名服务器 B. 辅域名服务器
C. 缓存域名服务器 D. 转发域名服务器

试题 3

以下关于 DNS 服务器的叙述中, 错误的是____(3)____。

(3) A. 用户只能使用本网段内 DNS 服务器进行域名解析
B. 主域名服务器负责维护这个区域的所有域名信息
C. 辅助域名服务器作为主域名服务器的备份服务器提供域名解析服务
D. 转发域名服务器负责非本地域名的查询

试题 4

在以下域名服务器中, 没有域名数据库的是____(4)____。

(4) A. 缓存域名服务器 B. 主域名服务器
C. 辅域名服务器 D. 转发域名服务器

试题 5

通过“Internet 信息服务 (IIS) 管理器”管理单元可以配置 FTP 服务, 若将控制端口设置为 2222, 则数据端口自动设置为____(5)____。

(5) A. 20 B. 80 C. 543 D. 2221

试题 6

某 Linux DHCP 服务器 dhcpd.conf 的配置文件如下:

```
ddns-update-style none;  
subnet 192.168.0.0 netmask 255.255.255.0 {  
range 192.168.0.200 192.168.0.254;  
ignore client-updates;  
default-lease-time 3600;  
max-lease-time 7200;  
option routers 192.168.0.1;  
option domain-name "test.org";  
option domain-name-servers 192.168.0.2;
```

```
}  
host test 1 {hardware ethernet 00:E0:4C:70:33:65;fixed-address 192.168.0.8;}
```

客户机 IP 地址的默认租用期为____(6)____小时。

- (6) A. 1 B. 2 C. 60 D. 120

试题 7

DHCP 客户机不能从 DHCP 服务器获得____(7)____。

- (7) A. DHCP 服务器的 IP 地址 B. Web 服务器的 IP 地址
C. DNS 服务器的 IP 地址 D. 默认网关的 IP 地址

试题 8

在 IIS 服务支持的身份验证方法中，需要利用明文在网络上传递用户名和密码的是____(8)____。

- (8) A. NET Passport 身份验证 B. 集成 Windows 身份验证
C. 基本身份验证 D. 摘要式身份验证

试题 9

在 Linux 操作系统中，网络管理员可以通过修改____(9)____文件对 Web 服务器端口进行配置。

- (9) A. inetd.conf B. lilo.conf C. httpd.conf D. resolv.conf

试题 10

在 Windows Server 2003 上启用 IIS 6.0 提供 Web 服务，创建一个 Web 站点并将主页文件 index.asp 复制到该 Web 站点的主目录下。在客户机的浏览器地址栏内输入网站的域名后提示没有权限访问该网站，则可能的原因是____(10)____。

- (10) A. 没有重新启动 Web 站点
B. 没有在浏览器上指定该 Web 站点的服务端口 80
C. 没有将 index.asp 添加到该 Web 站点的默认启动文档中
D. 客户机安装的不是 Windows 操作系统

试题 11

FTP 客户上传文件时，通过服务器 20 端口建立的连接是____(11)____，FTP 客户端应用进程的端口可以为____(12)____。

- (11) A. 建立在 TCP 之上的控制连接 B. 建立在 TCP 之上的数据连接
C. 建立在 UDP 之上的控制连接 D. 建立在 UDP 之上的数据连接
(12) A. 20 B. 21 C. 80 D. 4155

试题 12

为保证在启动 Linux 服务器时自动启动 DHCP 进程，应在____(13)____文件中将配置项 dhcpd=no 改为 dhcpd=yes。

- (13) A. /etc/rc.d/rc.inet1 B. /etc/rc.d/rc.inet2
C. /etc/dhcpd.conf D. /etc/rc.d/rc.s

试题 13

在 Windows 操作系统下可以通过安装____(14)____组件来提供 FTP 服务。

- (14) A. IIS B. IE C. Outlook D. Apache

试题 14

Windows Server 2003 中的 IIS 为 Web 服务提供了许多选项，利用这些选项可以更好地配

置 Web 服务的性能、行为和安全等。如图 12-49 所示,“限制网络带宽”选项属于 (15) 选项卡。

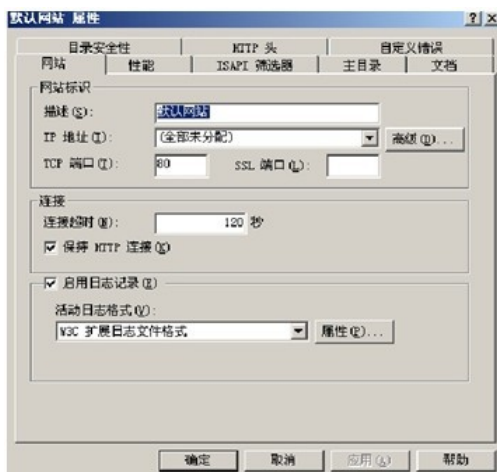


图 12-49 站点属性

- (15) A. HTTP 头 B. 性能 C. 主目录 D. 文档

试题 15

若 Linux 用户需要将 FTP 默认的 21 号端口修改为 8800,可以修改 (16) 配置文件。

- (16) A. /etc/vsftpd/userconf B. /etc/vsftpd/vsftpd.conf
C. /etc/resolv.conf D. /etc/hosts

试题 16

在 Windows Server 2003 的“管理您的服务器”界面中,可以通过 (17) 安装配置 DHCP 服务器。

- (17) A. Active Directory B. 管理服务器角色
C. IIS 6.0 D. 代理服务器

试题 17

用户可以通过 http://www.a.com 和 http://www.b.com 访问在同一台服务器上 (18) 不同的两个 Web 站点。

- (18) A. IP 地址 B. 端口号 C. 协议 D. 虚拟目录

试题 18

要使 Samba 服务器在网上邻居中出现的主机名为 smbserver,其配置文件 smb.conf 中应包含 (19)。

- (19) A. workgroup=smbserver B. netbios name=smbserver
C. server string=smbserver D. guest account=smbserver

试题 19

某 Apache 服务器的配置文件 httpd.conf 包含如下所示配置项。在 (20) 处选择合适的选项,使得用户可通过 http://www.test.cn 访问到该 Apache 服务器;当用户访问 http://111.25.4.30:80 时,会访问到 (21) 虚拟主机。

```
NameVirtualHost 111.25.4.30: 80
ServerName www.othertest.com
DocumentRoot /www/othertest
```

```
ServerName (32)
DocumentRoot /www/otherdate
ServerName www.test.com
ServerAlias test.com *.test.com
DocumentRoot /www/test
```

(20) A. www.othertest.com

B. www.test.com

C. www.test.cn

D. ftp.test.com

(21) A. www.othertest.com

B. www.test.com

C. www.test.cn

D. ftp.test.com

试题 20

在配置 IIS 时, 如果想禁止某些 IP 地址访问 Web 服务器, 应在“默认 Web 站点”的属性对话框中, (22) 选项卡中进行配置。

(22) A. 目录安全性

B. 文档

C. 主目录

D. ISAPI 筛选器

12.8 习题解析

试题 1 分析

DNS 每个区域数据库文件都是由资源记录构成的。主要有: SOA 记录、NS 记录、A 记录、CNAME 记录、MX 记录和 PTR 记录。其中 A 记录也称为主机记录, 是 DNS 名称到 IP 地址的映射, 用于正向解析。

试题 1 答案

(1) C

试题 2 分析

本试题考查 DNS 服务器的解析机制。

通常由主域名服务器、辅域名服务器、缓存域名服务器、转发域名服务器进行域名解析。主域名服务器负责维护这个区域的所有域名信息, 需要从域管理员构造的本地磁盘文件中加载域信息进行解析。辅助域名服务器作为主域名服务器的备份服务器提供域名解析服务。辅助服务器从主域名服务器获得授权, 有一个所有域信息的完整备份, 解析时需要访问本地存储文件。缓存域名服务器可运行域名服务器软件但是没有域名数据库, 它从某个远程服务器取得每次域名服务器查询的回答, 一旦取得一个答案, 就把它放在高速缓存中, 以后查询相同的信息时就用它予以回答。转发域名服务器负责所有非本地域名的本地查询, 转发域名服务器接到查询请求时, 在其缓存中查找, 如找不到就把请求依次转发到指定的域名服务器, 直到查询到结果为止, 否则返回无法映射的结果。

从上述服务器的查询机制中可以看出, 缓存域名服务器通过高速缓存的存取进行域名解析, 因此获取的解析结果耗时最短。

试题 2 答案

(2) C

试题 3 分析

主域服务器: 具有一个或几个域区的授权, 并负责维护这个区域的所有域名信息。辅助域名服务器作为主域名服务器的备份服务器也同样提供域名解析服务。而转发域名服务器主要负责非本地域名的查询。由于域名结构在整个 Internet 中是一个树形结构, 通过递归查询或者迭代查询方式来查找域名, 因此任何一个 Internet 用户可以使用整个域名树上的任何一个域名服务器来解析域名。

试题 3 答案

(3) A

试题 4 分析

主域服务器：具有一个或几个域区的授权。域区就是一个或几个域的数据，也可以是一个域的部分数据。并且一个域只能有一个主域名服务器。

辅助域名服务器：也具有授权功能，作为主域名服务器的备份。它通过域区传送从主服务器获得所有的域区数据。

缓存域名服务器：通过自己的查询操作建立地址缓存的服务器。只用于缓存的服务器，没有自己的域区数据，只为客户机进行查询。

试题 4 答案

(4) A

试题 5 分析

正常情况下，FTP 需要两个端口对外传输，如果你使用默认的 21，还需要 20 端口传输数据，也就是说，数据传输端口比控制端口小 1，例如，你把 FTP 的端口改为 2222，则数据传输的端口就是 2221 了。这道题首先可以排除 B 和 C 选项。

另外要注意的一个问题就是 FTP 服务器的模式问题。

主动方式 FTP 的主要问题实际上在于客户端。FTP 的客户端并没有实际建立一个到服务器数据端口的连接，它只是告诉服务器自己监听的一个随机端口号，服务器再回来连接客户端这个指定的端口。

被动 FTP 也称为 PASV 模式，只有当客户端通知服务器它处于被动模式时才启用。

在被动方式 FTP 中，命令连接和数据连接都是由客户端发起的，当开启一个 FTP 连接时，客户端打开两个任意的非特权本地端口 ($N > 1024$ 和 $N+1$)。第一个端口连接服务器的 21 端口，但与主动方式的 FTP 不同，客户端不会提交 PORT 命令并允许服务器来回连它的数据端口，而是提交 PASV 命令。这样做的结果是服务器会开启一个任意的非特权端口 ($P > 1024$)，并发送 PORT P 命令给客户端。然后客户端发起从本地端口 $N+1$ 到服务器的端口 P 的连接用来传送数据。

简单来说就是下面的这个模型。

① 主动 FTP

命令连接：客户端 > 1024 端口 \rightarrow 服务器 21 端口。

数据连接：客户端 > 1024 端口 \rightarrow 服务器 20 端口。

② 被动 FTP

命令连接：客户端 > 1024 端口 \rightarrow 服务器 21 端口。

数据连接：客户端 > 1024 端口 \rightarrow 服务器 > 1024 端口。

试题 5 答案

(5) D

试题 6 分析

从配置文件 default-lease-time 3600 即可知道，默认的租期是 $3600/60 \times 60 = 1$ 小时。

试题 6 答案

(6) A

试题 7 分析

DHCP 服务器通过 option 可以指定给客户端对应的一些 IP 配置信息。如 DNS 服务器地

址，默认网关地址等。但是 Web 服务器地址与 DHCP 并没有什么直接的联系。因此此题选择 B。

试题 7 答案

(7) B

试题 8 分析

Passport 验证是微软公司提供的一种集中式验证服务，与集成的 Windows 身份验证类似，用户名和密码都不采用明文传送。摘要式身份验证传送的用户和密码信息是信息的摘要，而不是明文的信息。只有基本身份验证采用明文的形式。

试题 8 答案

(8) C

试题 9 分析

本题考查 Linux 系统中 Web 服务器端口配置相关知识。

在 Linux 系统中，很多服务的配置数据都保存在相应的配置文件中（文件名一般为 server-name.conf）。

inetd.conf 是 /usr/sbin/inetd 的初始化文件，告诉 /usr/sbin/inetd 所需要监听的 inet 服务及有关信息，主要的信息有服务名称、协议（tcp 或 udp），标志（wait 或 nowait）、属主、真实服务程序全路径、真实服务程序名称及参数。lilo.conf 是 Linux 中多引导程序 lilo 的配置文件；resolv.conf 是 DNS 域名解析服务的配置文件。

httpd.conf 是 Linux 中 Apache Web 服务的配置文件，其中的 Listen 选项用于配置服务的 IP 地址和端口号。例如，Listen 192.168.1.1:8080 指定 Web 服务的 IP 地址为 192.168.1.1，端口号为 8080。

试题 9 答案

(9) C

试题 10 分析

默认文档是 Web 服务器收到一个请求时发送的一个文件。默认文档可以是一个网站，也可以是显示站点或文件夹内容的超文本列表的一个索引页面的主页。

配置 Web 服务器时，可以指定多个 Web 站点或文件夹为默认文档。IIS 搜索时，依据默认文档的顺序，返回它所发现的第一个文档。如果找到匹配项，IIS 将激活该站点或文件夹，返回文件夹列表。如果文件夹浏览未被激活，IIS 向浏览器返回“HTTP Error 403-禁止访问”消息。默认文档名称示例包括 default.htm、default.asp 和 index.htm 等。

试题 10 答案

(10) C

试题 11 分析

与大多数 Internet 服务一样，FTP 也采用客户机-服务器模式，客户机与服务器之间利用 TCP 建立连接。与其他客户机-服务器模式不同，FTP 客户机和服务器之间要建立双重连接，一个是控制连接，一个是数据连接。数据连接用于传输数据，当客户机通过控制连接向服务器发出数据传输命令时，便在客户机与服务器之间建立一条数据连接。数据连接建立成功后，开始数据传输，数据传输完成后，数据连接断开。

数据连接的建立有两种模式，即主动模式（Active）和被动模式（Passive）。主动模式（一般认为默认模式）：当客户机向服务器发出数据传输命令时，客户机在 TCP 的一个随机端口上被动打开数据传输进程，并通过控制连接利用 PORT 命令将客户机的数据传输进程所使用

的端口号发送给服务器，服务器在 TCP 的端口 20 上建立一个数据传输进程，并与客户机的数据传输进程建立数据连接。被动模式：当客户机向服务器发出数据传输命令时，通过控制连接向服务器发送一个 PASV 命令，请求进入被动模式。服务器在 TCP 的一个端口上 20 被动打开数据传输进程，并通过对 PASV 命令的响应将服务器数据传输进程使用的端口通知给客户机。客户机在 TCP 的一个随机端口上以主动方式打开数据传输进程，与服务器端的数据传输进程之间建立数据连接。

注：解析中提到了随机端口。因为 1024 以下端口已经被特定服务占用，例如 http 占用 TCP 80 端口，通常随机端口都指的是 1024 以上的端口。

试题 11 答案

(11) B

(12) D

试题 12 分析

Linux 系统中 TCP/IP 网络配置通过/etc/rc.d/rc.inet1 和/etc/rc.d/rc.inet2 两个文件来实现。/etc/rc.d/rc.inet1 主要是通过 ifconfig 和 route 命令进行基本的 TCP/IP 接口配置，主要由两个部分组成，第一部分是对回送接口的配置，第二部分是对以太网接口的配置。而/etc/rc.d/rc.inet2 主要是用来启动一些网络监控的进程，如 inetd portmapper 等。

试题 12 答案

(13) A

试题 13 分析

在 Windows 系统中，IIS 可以提供包括 WWW、FTP 等多种网络服务，IE 可以用来访问各种网络服务，Outlook 可以用来接收和发送电子邮件，Apache 可以用来架设 WWW 站点，因此答案选 A。

试题 13 答案

(14) A

试题 14 分析

本题考查 Windows Server 2003 中 IIS 的选项，属于记忆题。“限制网络带宽”选项属于“性能”选项卡。

试题 14 答案

(15) B

试题 15 分析

VSFTPD 的配置文件/etc/vsftpd/vsftpd.conf 是一个文本文件。以“#”字符开始的行是注释行。每个选项设置为一行，格式为“option=value”，注意“=”号两边不能留空白符。除了这个主配置文件外，还可以给特定用户设定个人配置文件。

VSFTPD 包中所带的 vsftpd.conf 文件配置比较简单。我们可以根据实际情况对其进行一些设置，以使得 VSFTPD 更加可用。

监听地址与控制端口：

```
listen address=ip address
```

此参数在 VSFTPD 使用单独 (standalone) 模式下有效。此参数定义了在主机的哪个 IP 地址上监听 FTP 请求，即在哪个 IP 地址上提供 FTP 服务。对于只有一个 IP 地址的主机，不需要使用此参数。对于多址主机，不设置此参数，则监听所有 IP 地址。默认值为无。

```
listen_port=port_value
```

指定 FTP 服务器监听的端口号（控制端口），默认值为 21。此选项在 standalone 模式下生效。

FTP 模式与数据端口

FTP 分为两类：PORT FTP 和 PASV FTP。PORT FTP 是一般形式的 FTP。这两种 FTP 在建立控制连接时操作是一样的，都是由客户端首先和 FTP 服务器的控制端口（默认值为 21）建立控制链接，并通过此链接进行传输操作指令。它们的区别在于使用数据传输端口的方式。PORT FTP 由 FTP 服务器指定数据传输所使用的端口，默认值为 20。PASV FTP 由 FTP 客户端决定数据传输的端口。PASV FTP 这种做法主要是考虑到存在防火墙的环境下，由客户端与服务器进行沟通（客户端向服务器发出数据传输请求中包含了数据传输端口），决定两者之间的数据传输端口更为方便一些。

```
port enable=YES | NO
```

在数据连接时取消 PORT 模式，设此选项为 NO。它的默认值为 YES。

```
connect_from_port 20=YES | NO
```

控制以 PORT 模式进行数据传输时是否使用 20 端口（ftp-data）。YES 为使用，NO 为不使用。默认值为 NO，但 RHL 自带的 vsftpd.conf 文件中此参数设为 YES。

试题 15 答案

(16) B

试题 16 分析

可以通过管理服务角色来安装配置 DHCP 服务器。

试题 16 答案

(17) B

试题 17 分析

本题考查的是 IIS 下多站点的配置。

在 IIS 下配置多站点时，可以采用虚拟主机和虚拟目录两种方式。

采用虚拟目录时，发布的站点没有独立域名，而是在主域名下建立虚拟目录，从题目要求看，需要两个独立的域名，所以不可实现。

采用虚拟主机时有三种方式，即使用不同 IP 地址，不同端口号和不同的主机头。

使用不同 IP 地址时要求 Web 服务器配备多网卡，使用不同端口号时，要求在访问 Web 服务器虚拟主机时指名端口号，例如：http://www.b.com:8080，使用不同主机头时，在 IIS 发布中要做主机头域名指定。

从题目选项中可见，只有 A 选项符合要求。

试题 17 答案

(18) A

试题 18 分析

本题考查 Samba 服务器的配置知识。

在 Samba 服务器配置文件 smb.conf 中，workgroup 项表示在 Windows 操作系统中的“网上邻居”中将会出现的 Samba 服务器所属群组，默认为 MYGROUP，不区分大小写。server string 项是 Samba 服务器的注释说明。netbios name 项定义 netbios 名字，其名字在“网上邻居”中出现。guest account 项设定访问 samba server 的来宾账户（即访问时不用输入用户名和密码的账户），若设为 pcguest，则默认为 nobody 用户。

试题 18 答案

(19) B

试题 19 分析

本题考查 Apache 服务器的配置。

在 Apache 服务器的配置文件 httpd.conf 中，NameVirtualHost 用来指定虚拟主机使用的 IP 地址，这个 IP 地址将对应多个 DNS 名字。如果 Apache 使用了 Listen 参数控制了多个端口，那么就可以在这里加上端口号以进一步进行区分对不同端口的不同连接请求。此后，使用 VirtualHost 语句，使用 NameVirtualHost 指定的 IP 地址作为参数，对每个名字都定义对应的虚拟主机设置。

按照题目要求，用户可通过 `http://www.test.cn` 访问到该 Apache 服务器，而配置文件中 ServerName 缺少 `www.test.cn`，所以空 (21) 处应填写 `www.test.cn`，当用户访问 `http://111.25.4.30:80` 时，会访问配置文件中定义的第一个虚拟主机 `www.othertest.com`。

试题 19 答案

(20) C

(21) A

试题 20 分析

本题考查 IIS 的配置知识。在配置 IIS 时，如果想禁止某些 IP 地址访问 Web 服务器，应在“默认 Web 站点属性”对话框中“目录安全性”选项卡的“IP 地址及域名限制”选项区域中配置。

试题 20 答案

(22) A

网络工程师案例分析

举办网络工程师考试的目的是使得通过本考试的合格人员能根据应用部门的要求进行网络系统的规划、设计和网络设备的软硬件安装调试工作，能进行网络系统的运行、维护和管理，能高效、可靠、安全地管理网络资源，作为网络专业人员对系统开发进行技术支持和指导，具有工程师的实际工作能力和业务水平，能指导网络管理员从事网络系统的构建和管理工作。

与软件考试中其他科目一样，网络工程师考试除了要求考生具备扎实的理论基础外，还需要有一定的实际操作能力、故障排除能力，特别是对各种服务器配置、路由交换机配置实际操作能力提出了更多的要求。有实际施工经验的考生学习下午知识模块时，其工作经验会让学习事半功倍。

任何认证考试的宗旨不是为了考试而考试，而是为了在考试中系统地学习相关的知识，并把所学知识灵活运用到实际的工作中，达到学以致用目的。

13.1 考点脉络

目前网络工程师考试是根据最新 2009 版考试大纲的要求命题的。计算机与网络知识作为综合题出现在上午考题中，其知识点的详细讲解已经在前面第 1~12 章涉及。本章主要讨论的是网络系统的设计与管理这一大体知识模块的考题分析，这一般都是出现网络工程师考试的下午题部分。网络系统设计与管理依据 2009 版网络工程师考试的考试大纲，主要分为网络系统的分析与设计、网络系统的运维和管理、网络系统实现技术、网络新技术四个部分。其中网络系统的实现技术涉及可靠性设计、网络设备、网络应用于服务、网络安全四个知识点。下午题考题通常都是隶属于这四个知识点，所以网络系统的实现技术部分是下午考题中的重中之重。如表 13-1 所示是 2010 年至 2012 年 8 次考试中下午题部分的汇总明细。

表 13-1 下午题考题汇总

年 份	试 题	知 识 点	分 值
2010 年上半年	试题一	网络系统分析与设计	15 分
	试题二	网络系统实现（Linux 下 Xinetd 服务）	15 分
	试题三	网络系统实现（Windows 下终端服务器）	15 分
	试题四	网络系统实现（Windows 下安全策略）	15 分
	试题五	网络系统实现（ISATAP 隧道）	15 分
2010 年下半年	试题一	网络系统分析与设计	15 分
	试题二	网络系统实现（Linux 系统网络设置）	15 分
	试题三	网络系统实现（Windows 系统 Web、FTP 服务器设置）	15 分
	试题四	网络系统实现（Windows VPN 服务器设置）	15 分
	试题五	网络系统实现（GRE 隧道技术）	15 分

续表

年 份	试 题	知 识 点	分 值
2011 年上半年	试题一	网络系统分析与设计	15 分
	试题二	网络系统实现（Linux 系统管理）	15 分
	试题三	网络系统实现（Windows 下 DHCP、Web、FTP 服务器设置）	15 分
	试题四	网络系统实现（IPsec VPN 设置）	15 分
	试题五	网络系统实现（路由与 ACL 配置）	15 分
2011 年下半年	试题一	网络系统分析与设计	15 分
	试题二	网络系统实现（Linux 下 Apache 服务器设置）	15 分
	试题三	网络系统实现（Windows 下 DNS 服务器设置）	15 分
	试题四	网络系统实现（ACL 设置）	15 分
	试题五	网络系统实现（IPv6 NAT-PT 过渡技术）	15 分
2012 年上半年	试题一	网络系统分析与设计	15 分
	试题二	网络系统实现（Linux 下 DHCP 服务器配置技术）	15 分
	试题三	网络系统实现（Windows 下 DNS 服务器配置技术）	15 分
	试题四	网络系统实现（Windows 下 IPsec 配置技术）	15 分
	试题五	网络系统实现（路由器 VPN 配置技术）	15 分
2012 年下半年	试题一	网络系统分析与设计	20 分
	试题二	网络系统实现（Linux 下 FTP 服务器配置技术）	15 分
	试题三	网络系统实现（Windows 服多种务器配置）	20 分
	试题四	网络系统实现（网络设备常用配置命令）	15 分

13.2 考前冲刺

以下列举了历年网络工程师考试中出题频率较高的试题类型，分别是网络系统分析与设计类、Linux 服务器配置类、Windows 服务器配置类、网络设备配置（路由器、交换机、防火墙）类。

试题一（共 15 分）

阅读以下说明，回答问题 1 至问题 4，将解答填入答题纸对应的解答栏内。

【说明】

某校园网拓扑结构如图 13-1 所示。

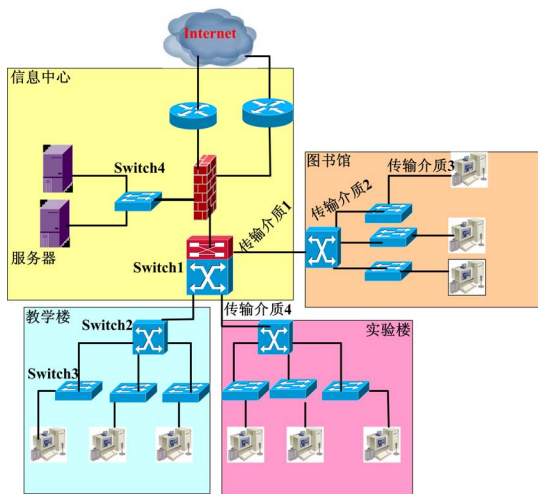


图 13-1 某校园网拓扑结构图

该网络中的部分需求如下。

1. 信息中心距图书馆 2 千米，距教学楼 300 米，距实验楼 200 米。
2. 图书馆的汇聚交换机置于图书馆主机房内，楼层设备间共有两个，分别位于二层和四层，距图书馆主机房距离均大于 200 米，其中，二层设备间负责一、二层的计算机接入，四层设备间负责三~五层的计算机接入，各层信息点数如表 13-2 示。

表 13-2 楼层信息点分布情况

楼 层	信 息 点 数
1	24
2	24
3	19
4	21
5	36

3. 所有计算机采用静态 IP 地址。
4. 学校网络要求千兆干线，百兆到桌面。
5. 信息中心有两条百兆出口线路，在防火墙上根据外网 IP 设置出口策略，分别从两个出口访问 Internet。
6. 信息中心共有多台服务器，通过交换机接入防火墙。
7. 信息中心提供的信息服务包括 Web、FTP、数据库、流媒体等，数据流量较大，要求千兆接入。

【问题 1】（4 分）

根据网络的需求和拓扑图，在满足网络功能的前提下，本着最节约成本的布线方式，传输介质 1 应采用__（1）__，传输介质 2 应采用__（2）__，传输介质 3 应采用__（3）__，传输介质 4 应采用__（4）__。

（1）~（4）备选答案：

- A. 单模光纤 B. 多模光纤 C. 基带同轴电缆
D. 宽带同轴电缆 E. 1 类双绞线 F. 5 类双绞线

【问题 2】（6 分）

学校根据网络需求选择了四种类型的交换机，其基本参数如表 13-3 所示。

表 13-3 交换机类型

交换机类型	参 数
A	12 个固定千兆 RJ45 接口，背板带宽—24Gb/s，包转发率—18Mpps
B	24 个千兆 SFP，背板带宽—192Gb，包转发率—150Mpps
C	模块化交换机，背板带宽—1.8Tb，包转发率—300Mpps，业务插槽数量—8 个，支持电源冗余
D	24 个固定百兆 RJ45 接口，1 个 GBIC 插槽，包转发率—7.6Mpps

根据网络需求、拓扑图和交换机参数类型，在图 13-1 中，Switch1 应采用__（5）__类型交换机，Switch2 应采用__（6）__类型交换机，Switch3 应采用__（7）__类型交换机，Switch4 应采用__（8）__类型交换机。

根据需求描述和所选交换机类型，图书馆二层设备间最少需要交换机__（9）__台，图书馆四层设备间最少需要交换机__（10）__台。

【问题 3】（3 分）

该网络采用核心层、汇聚层、接入层的三层架构。根据层次化网络设计的原则，数据包过滤、协议转换应在__（11）__层完成。__（12）__层提供高速骨干线路，MAC 层过滤和

IP 地址绑定应在__（13）__层完成。

【问题 4】（2 分）

根据该网络的需求，防火墙至少需要__（14）__个百兆接口和__（15）__个千兆接口。

试题二（共 15 分）

阅读以下关于 Linux 文件系统和 Samba 服务的说明，回答问题 1 至问题 3。

【说明】

Linux 系统采用了树形多级目录来管理文件，树形结构的最上层是根目录，其他所有目录都是从根目录生成的。

通过 Samba 服务可以实现基于 Linux 操作系统的服务器和基于 Windows 操作系统的客户机之间的文件、目录及共享打印服务。

【问题 1】（6 分）

Linux 在安装时会创建一些默认的目录，如表 13-4 所示。

表 13-4 Linux 根目录的作用

/	
/bin	
/boot	存放启动系统使用的文件
/dev	
/etc	用来存放系统管理所需要的配置文件和子目录
/home	
/lib	文件系统中程序所需要的共享库
/lost+found	
/mnt	临时安装（mount）文件系统的挂载点
/opt	
/proc	
/root	
/sbin	
/usr	
/var	包含系统运行时要改变的数据
/tmp	

依据表 13-4，在（1）～（6）处填写恰当的内容（其中（1）在候选答案中选择）。

① 对于多分区的 Linux 系统，文件目录树的数目是__（1）__。

② Linux 系统的根目录是__（2）__，默认的用户主目录在__（3）__目录下，系统的设备文件（如打印驱动）存放在__（4）__目录中，__（5）__目录中的内容关机后不能被保存。

③ 如果在工作期间突然停电，或者没有正常关机，在重新启动机器时，系统将要复查文件系统，系统将找到的无法确定位置的文件放到目录__（6）__中。

（1）备选答案：

A. 1 B. 分区的数目 C. 大于 1

【问题 2】（4 分）

默认情况下，系统将创建的普通文件的权限设置为-rw-r--r--，即文件所有者对文件__（7）__，同组用户对文件__（8）__，其他用户对文件__（9）__。文件的所有者或者超级用户，采用__（10）__命令可以改变文件的访问权限。

【问题 3】（5 分）

在 Linux 系统中 Samba 的主要配置文件是/etc/samba/smb.conf。请根据以下的 smb.conf

配置文件，在（11）～（15）处填写恰当的内容。

Linux 服务器启动 Samba 服务后，在客户机的“网络邻居”中显示提供共享服务的 Linux 主机名为（11），其共享的服务有（12），能够访问 Samba 共享服务的客户机的地址范围（13）；能够通过 Samba 服务读 / 写/home/samba 中内容的用户是（14）；该 Samba 服务器的安全级别是（15）。

```
[global]
workgroup = MYGROUP
netbios name=smb-server
server string = Samba Server
;hosts allow = 192.168.1. 192.168.2. 127.
load printers = yes
security = user
[printers]
comment = My Printer
browseable = yes
path = /usr/spool/samba
guest ok = yes
writable = no
printable = yes
[public]
comment = Public Test
browseable = no
path = /home/samba
public = yes
writable = yes
printable = no
write list = @test
[user1dir]
comment = User1's Service
browseable = no
path = /usr/user1
valid users = user1
public = no
writable = yes
printable = no
```

试题三（共 15 分）

阅读以下说明，回答问题 1 至问题 3，将答案填入答题纸对应的解答栏内。

【说明】

在大型网络中，通常采用 DHCP 完成基本网络配置会更有效率。

【问题 1】（1 分）

在 Linux 系统中，DHCP 服务默认的配置文件的（1）。

（1）备选答案：

- | | |
|--------------------|----------------------|
| A. /etc/dhcpd.conf | B. /etc/dhcpd.config |
| C. /etc/dhcp.conf | D. /etc/dhcp.config |

【问题 2】（4 分）

管理员可以在命令行通过（2）命令启动 DHCP 服务；通过（3）命令停止 DHCP 服务。

（2）和（3）备选答案：

- | | |
|------------------------|-----------------------|
| A. service dhcpd start | B. service dhcpd up |
| C. service dhcpd stop | D. service dhcpd down |

【问题 3】（10 分）

在 Linux 系统中配置 DHCP 服务器，该服务器配置文件的部分内容如下：

```
subnet 192.168.1.0 netmask 255.255.255.0 {
```

```

option routers 192.168.1.254;
option subnet-mask 255.255.255.0;
option broadcast-address 192.168.1.255;
option domain-name-servers 192.168.1.3;
range 192.168.1.100 192.168.1.200;
default-lease-time 21600;
max-lease-time 43200;

host webserver {
    hardware ethernet 52:54:AB:34:5B:09;
    fixed-address 192.168.1.100;
}
}

```

在主机 webserver 上运行 ifconfig 命令时显示如图 13-2 所示，根据 DHCP 配置，填写空格中缺少的内容。

```

eth0      Link encap:Ethernet  HWaddr (4)
          inet addr: (5)  Bcast:192.168.1.255  Mask: (6)
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:4 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:0 (0.0 b)  TX bytes:168 (168.0 b)
          Interrupt:10 Base address:0x10a4

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:397 errors:0 dropped:0 overruns:0 frame:0
          TX packets:397 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:26682 (26.0 Kb)  TX bytes:26682 (26.0 Kb)

```

图 13-2 ifconfig 命令运行结果

该网段的网关 IP 地址为 (7)，域名服务器 IP 地址为 (8)。

试题四（共 15 分）

阅读以下说明，回答问题 1 至问题 5，将答案填入答题纸对应的解答栏内。

【说明】

某网络拓扑结构如图 13-3 所示，网络 1 和网络 2 的主机均由 DHCP_Server 分配 IP 地址。FTP_Server 的操作系统为 Windows Server 2003，Web_Server 的域名为 www.csairk.com。

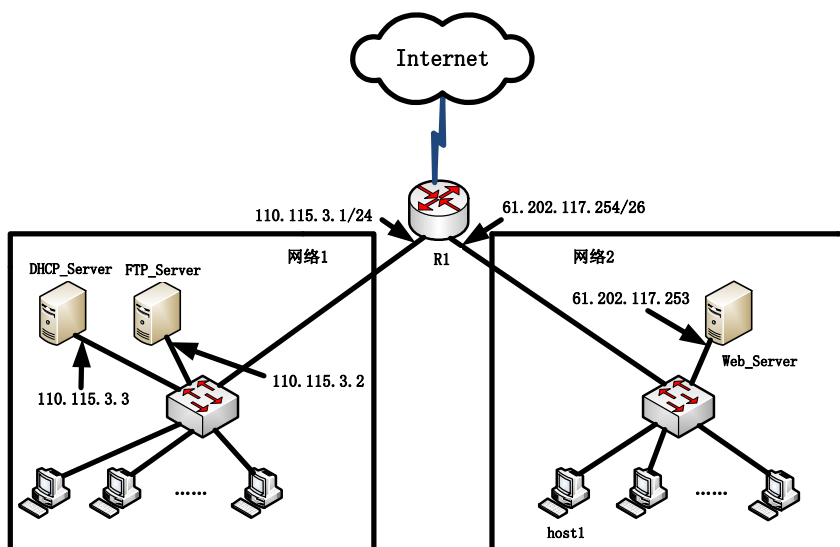


图 13-3 某网络拓扑结构

【问题 1】(4 分)

DHCP Server 服务器可动态分配的 IP 地址范围为____(1)____和____(2)____。

【问题 2】(2 分)

若在 host 1 上运行 ipconfig 命令, 获得如图 13-4 所示结果, host 1 能正常访问 Internet 吗? 说明原因。

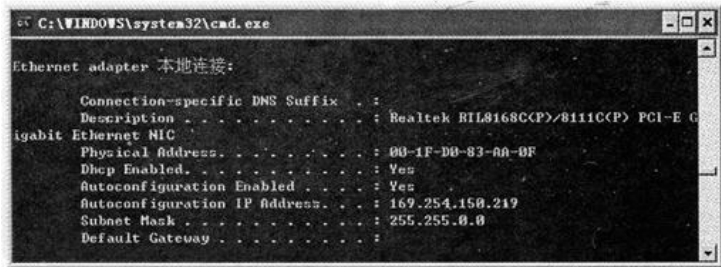


图 13-4 ipconfig 命令运行结果

【问题 3】(3 分)

若 host 1 成功获取 IP 地址后, 在访问 http://www.abc.com 网站时, 总是访问到 www.csairk.com, 而同一网段内的其他客户端访问该网站正常。在 host 1 的 C:\WINDOWS\system32\drivers\etc 目录下打开____(3)____文件, 发现其中有如下两条记录:

127. 0. 0. 1 localhost

____(4)____ www.abc.com

在清除第 2 条记录后关闭文件, 重启系统后 host 1 访问 http://www.abc.com 网站正常。请填写(4)处空缺内容。

【问题 4】(2 分)

在配置 FTP server 时, 应在图 13-5 中“IP 地址”文本框中填入____(5)____。

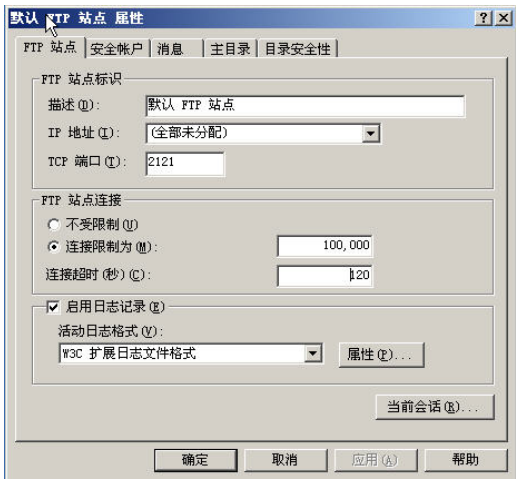


图 13-5 设置 IP 地址

【问题 5】(4 分) 若 FTP 配置的虚拟目录为 pcn, 虚拟目录配置如图 13-6 和图 13-7 所示。

根据以上配置, 哪些主机可访问该虚拟目录? 访问该虚拟目录的命令是____(6)____。

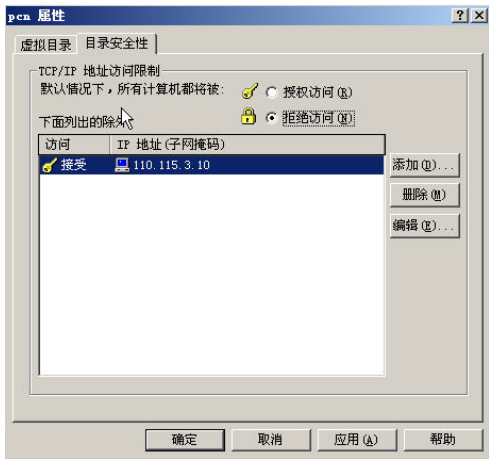


图 13-6 虚拟目录配置 1



图 13-7 虚拟目录配置 2

试题五（共 15 分）

阅读以下说明，回答问题 1 至问题 3，将答案填入答题纸对应的解答栏内。

【说明】

某单位采用双出口网络，其网络拓扑结构如图 13-8 所示。

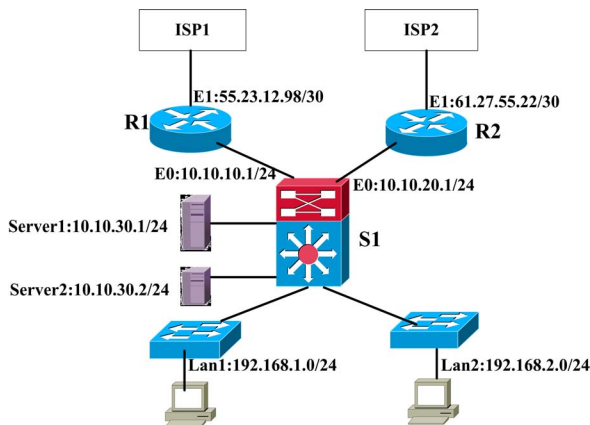


图 13-8 某单位网络拓扑图

该单位根据实际需要，配置网络出口实现如下功能：

1. 单位网内用户访问 IP 地址 158.124.0.0/15 和 158.153.208.0/20 时，出口经 ISP2；
2. 单位网内用户访问其他 IP 地址时，出口经 ISP1；
3. 服务器通过 ISP2 线路为外部提供服务。

【问题 1】（5 分）

在该单位的三层交换机 S1 上，根据上述要求完成静态路由配置。

```
ip route (1)
ip route 158.124.0.0 (2) (3)
ip route 158.153.208.0 (4) (5)
```

【问题 2】（6 分）

1. 根据上述要求，在三层交换机 S1 上配置了两组 ACL，请根据题目要求完成以下配置。

```
access -list 10 permit ip host 10.10.30.1 any
```

```
access -list 10 permit ip host (6) any
access -list 12 permit ip any 158.124.0.0 (7)
access -list 12 permit ip any 158.153.208.0 (8)
access -list 12 deny ip any any
```

2. 完成以下策略路由的配置。

```
route-map test permit 10
(9) ip address 10
(10) ip next-hop (11)
```

【问题 3】（4 分）

以下是路由器 R1 的部分配置。请完成配置命令。

```
R1(config)#interface fastethernet0/0
R1(config-if)#ip address (12) (13)
R1(config-if)ip nat inside
...
R1(config)#interface fastethernet0/1
R1(config-if)#ip address (14) (15)
R1(config-if)ip nat outside
...
```

13.3 习题解析

试题一分析

问题 1 解析

要解决本题 1 就要了解各类传输介质的传输特性，具体到本题就要熟悉单模光纤、多模光纤、基带同轴电缆、宽带同轴电缆、1 类双绞线、5 类双绞线的传输速率、传输长度。同时，要细致审题，因为题目给出了一个前提，即“在满足网络功能的前提下，本着最节约成本的布线方式”，因此既要考虑满足功能，又要考虑经济效益。

由于信息中心距图书馆 2 千米，超出了双绞线、多模光纤的有效传输距离，并且选项中的单模光纤传输距离是最长的，因此问题（1）答案为 A；图书馆的汇聚交换机置于图书馆主机房内，楼层设备间距图书馆主机房距离均大于 200 米，故不能选双绞线，且多模光纤比单模光纤便宜，因此问题（2）答案为 B；PC 到交换机，目前 5 类和超 5 类双绞线使用得最多，因此问题（3）答案为 F；信息中心距实验楼 200 米，因此问题（4）答案为 B。

问题 2 解析

要解决本题，需要了解交换机的几个相关参数。

① 背板带宽：是指交换机接口处理器或接口卡和数据总线间所能吞吐的最大数据量。背板带宽标志了交换机总的数据交换能力，也称交换带宽，一般的交换机的背板带宽从几 Gb/s 到上千 Gb/s 不等。一台交换机的背板带宽越高，所能处理数据的能力就越强，但同时设计成本也会越高。

一般的公式为：背板带宽=端口数×相应端口速率×2（全双工模式）。如果总带宽≤标称背板带宽，那么在背板带宽上是线速的。

② 包转发率

包转发率标志了交换机转发数据包能力的大小。单位一般为 pps（包每秒）。

计算公式如下：

包转发率=万兆端口数量×14.88Mpps+千兆端口数量×1.488Mpps+百兆端口数量×0.1488Mpps+其余类型端口数×相应计算方法。如果总速率能≤标称的包转发速率，那么交换

机在做第二层交换时可以做到线速。

这里以千兆包转发线速为例，解释 1.488Mpps 的由来。由于包转发线速的衡量标准是以单位时间内发送 64byte 的数据包（最小包）的个数作为计算基准的。对于千兆以太网来说，计算方法如下：

$$1\ 000\ 000\ 000\text{b/s}/8\text{bit}/(64+8+12)\text{byte}=1\ 488\ 095\text{pps}$$

说明：当以太网帧为 64byte 时，需考虑 8byte 的帧头和 12byte 的帧间隙的固定开销。故一个线速为千兆的以太网端口在转发 64byte 包时的包转发率为 1.488Mpps。

快速以太网的线速端口包转发率正好为千兆以太网的十分之一，为 148.8Kpps。万兆以太网，一个线速端口的包转发率为 14.88Mpps。千兆以太网，一个线速端口的包转发率为 1.488Mpps。对于快速以太网，一个线速端口的包转发率为 0.1488Mpps。

本题 Switch1 需要接入各子单位的千兆网络，需要处理大量数据，因此数据转发量很大。因此选择背板带宽=1.8Tb 的交换机类型 C；Switch2 属于汇聚层交换机，对背板带宽、包转发率要求较高，因此选择交换机类型 B；Switch3 属于接入层交换机，直接接 PC，对百兆接口需求量大，因此选择交换机类型 D；Switch4 接多台服务器，由于题目给出服务器流量较大，因此推断服务器均使用千兆的 RJ45 接口的网卡，因此选择交换机类型 A。

问题 3 解析

根据层次化网络设计的原则，数据包过滤、协议转换应在汇聚层完成；核心层提供高速骨干线路；MAC 层过滤和 IP 地址绑定在接入层完成。

问题 4 解析

在如图 13-1 所示的拓扑图中，没有明确防火墙具体位置，但实际上黑框代表的即为防火墙，接两个路由器通向不同的出口。信息中心有两条百兆出口线路，因此防火墙需要两个百兆接口。信息中心共有多台服务器，通过交换机接入防火墙，同时其他单位通过一个千兆口接入防火墙，因此防火墙需要两个千兆接口。

试题一参考答案

【问题 1】

(1) A (2) B (3) F (4) B

【问题 2】

(5) C (6) B (7) D (8) A (9) 2 (10) 4

【问题 3】

(11) 汇聚层 (12) 核心层 (13) 接入层

【问题 4】

(14) 2 (15) 2

试题二分析

问题 1 解析

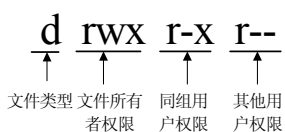
Linux 采用的是树形结构。最上层是根目录，其他所有目录都是从根目录出发而生成的。微软的 DOS 和 Windows 系统也是采用树形结构，但是在 DOS 和 Windows 中这样的树形结构的根是磁盘分区的盘符，有几个分区就有几个树形结构，它们之间的关系是并列的。但是在 Linux 中，无论操作系统管理几个磁盘分区，这样的目录树只有一个。Linux 根目录下各目录的描述和功能如 13-5 所示。

表 13-5 根目录下子目录描述

目 录 名	描 述
/	Linux 文件系统根目录
/bin	存放系统常用的可执行文件
/boot	存放 Linux 的内核以及系统启动文件
/dev	存放所有设备文件，包括硬盘、键盘、鼠标等
/etc	存放系统的所有配置文件
/home	用户主目录的默认位置
/lib	存放共享的库文件
/lost+found	系统非正常关机而留下“无家可归”的文件
/mnt	用于作为被挂载的文件系统的挂载点
/opt	作为可选文件和程序的存放目录
/proc	存放所有标志为进程的文件
/root	根用户的主目录
/sbin	存放更多的可执行文件
/usr	存放与系统用户直接有关的文件和目录
/var	通常用于存放长度可变的文件
/tmp	存放用户和程序的临时文件

问题 2 解析

在 Linux 系统中，每一个文件和目录都有相应的访问许可权限，文件或目录的访问权限分为可读（可列目录）、可写（对目录而言是可在目录中做写操作）和可执行（对目录而言是可以访问）三种，分别以 r、w 和 x 表示，其含义为：对于一个文件来说，可以将用户分成三种，即文件所有者、同组用户、其他用户，可对其分别赋予不同的权限。每一个文件或目录的访问权限都有三组，每组用三位表示，如图 13-9 所示。



注：文件类型有多种，d 代表目录，- 代表普通文件，c 代表字符设备文件。

更改文件的权限的命令为 **chmod**。

chmod 的语法格式为：

图 13-9 权限位示意图

chmod [who] [opt] [mode] 文件/目录名

其中 **who** 表示对象，是以下字母中的一个或组合：**u**（文件所有者）、**g**（同组用户）、**o**（其他用户）、**a**（所有用户）；**opt** 则代表操作，可以为+（添加权限）、-（取消权限）、=（赋予给定的权限，并取消原有的权限）；而 **mode** 则代表权限。

问题 3 解析

在 Linux 系统中 Samba 的主要配置文件是 `/etc/samba/smb.conf`。

smb.conf 文件有三个主要部分：

- ① 全局参数字段（**global**）：主机共享时的整体设置。
- ② 目录共享字段（**homes**）：定义一般参数，如建立共享文件目录等。
- ③ 打印机共享字段（**printers**）：打印机的配置和共享。

下面对 **smb.conf** 文件中的主要设置项进行逐一解释说明。

```
[global]
workgroup = MYGROUP
# 此参数设置服务器所要加入工作组的名称，系统默认为 MYGROUP
netbios name=smb-server
```



```

# 此参数在配置文件中未列出，需要手动添加，用于设置显示在“网上邻居”中的主机名
server string = Samba Server
# 此参数描述 Samba 服务器的一些信息，这些注释信息会显示在“网上邻居”中
;hosts allow = 192.168.1. 192.168.2. 127.
# 此参数设置哪些 IP 允许访问该服务器，本例中因为 hosts allow 被分号注释掉了，所以代表无限制
    load printers = yes          # 允许自动加载打印机列表
    security = user              # 设置 Samba 服务器的安全模式，本例中设置为用户安全级模式
    [printers]
    comment = My Printer        # 共享打印服务名称
    browseable = yes            # 设置是否允许浏览打印机
    path = /usr/spool/samba      # 设置打印机队列位置
    guest ok = yes              # 访问打印机是否需要密码
    writable = no               # 共享打印机必须设置 no
    printable = yes             # 是否允许打印
    [public]
    comment = Public Test       # 对共享目录的描述
    browseable = no             # 设置是否允许浏览目录
    path = /home/samba          # 设置共享目录位置
    public = yes                # 是否所用用户可访问
    writable = yes              # 用户是否有写的权限
    printable = no              # 是否允许打印
    write list = @test
# 允许写入权限的用户列表，此例中表示只有 test 组用户成员对该目录有写入的权限
    [userldir]
    comment = User1's Service   # 对个人目录的描述
    browseable = no             # 设置是否允许浏览目录
    path = /usr/usr1            # 设置共享目录位置
    valid users = user1         # 允许访问的用户列表
    public = no                 # 是否允许所有用户可访问
    writable = yes              # 用户是否有写的权限
    printable = no              # 是否允许打印

```

试题二参考答案

【问题 1】

- (1) A
- (2) /
- (3) /home
- (4) /dev
- (5) /proc
- (6) /lost+found

【问题 2】

- (7) 可读、可写
- (8) 仅可读
- (9) 仅可读
- (10) Chmod

【问题 3】

- (11) smb-servre
- (12) printers 或 My Printer
- (13) 无限制（因为 bosts allow 被分号注释掉了）
- (14) Linux 系统的 test 组中用户（仅回答 test 用户不给分）
- (15) 用户安全级

试题三分析

问题 1 解析

在 Linux 下配置 DHCP，主要工作是对相关文件进行解析。在 Linux 系统中，DHCP 服务默认的配置文件的 `/etc/dhcpd.conf`，它是一个递归下降格式的配置文件，有点像 C 语言的源程序风格，由参数和声明两大类语句构成，参数类语句主要告诉 DHCPd 网络参数，如租约时间、网关、DNS 等；而声明语句则用来描述网络的拓扑，表明网络上的客户，要提供给客户的 IP 地址，提供一个参数组给一组声明等。

问题 2 解析

可以使用以下命令来启动、停止和重启 DHCP 服务器程序：

```
[root@lib1 root] # service dhcpd [ start | stop | restart ]
```

或

```
[root@lib1 root] # etc/init.d/dhcpd [ start | stop | restart ]
```

其中 `start`、`stop`、`restart` 为任选参数，分别表示启动、停止和重启。执行以上命令启动后，DHCP 默认是启动在 `eth0` 上的，如果 DHCP 上的服务器还有另外一块网卡 `eth1`，想在 `eth1` 上启动 `dhcpd`，就输入：

```
[root@lib1 root] # /usr/sbin/dhcpd eth1
```

问题 3 解析

下面为 `dhcpd.conf` 配置文件中最常用和最重要的语句。

DHCP 配置语句如表 13-6 所示。

试题三参考答案

【问题 1】

(1) A

表 13-6 DHCP 配置语句

类型	语 句 格 式	功能与参数描述
标准参数类语句	<code>ddns-update-style type</code>	动态 DNS 解析方式，可选参数分别为： <code>ad-hoc</code> 、 <code>interim</code> 、 <code>none</code>
	<code>default-lease-time time</code>	指定默认租约时间，这里的 <code>time</code> 是以秒为单位的。如果 DHCP 客户在请求一个租约时没有指定租约的失效时间，租约时间就是默认租约时间
	<code>max-lease-time time</code>	最大的租约时间。如果 DHCP 在请求租约时间时发出特定的租约失效时间的请求，则用最大租约时间
	<code>Hardware hardware-type hardware-address</code>	指明物理硬件接口类型和硬件地址。硬件地址由 6 个 8 位组构成，每个 8 位组以 “:” 隔开。如 <code>00:00:E8:1B:54:97</code>
	<code>server-name “name”</code>	用于告知客户端所连接服务器的名字
	<code>fixed-address address [, address ...]</code>	用于指定一个或多个 IP 地址给一个 DHCP 客户，只能出现在 <code>host</code> 声明里
选项类语句	<code>option subnet-mask mask</code>	DHCP 服务配置子网掩码选项，服务开启后可应用于所有客户端
	<code>option broadcast-address IP 地址</code>	DHCP 服务配置广播地址选项，服务开启后可应用于所有客户端
	<code>option routers IP 地址</code>	同上，DHCP 服务配置网关（路由）地址选项，可设多个
	<code>option domain-name-servers IP 地址</code>	DHCP 服务配置 DNS 服务器地址，可应用于所有客户端，可设多个
	<code>option domain-name “csai.cn”</code>	DHCP 服务配置域名服务，可应用于所有客户端
	<code>option host-name string</code>	给客户指定主机名， <code>string</code> 是一个字符串

【问题 2】

- (2) A
- (3) C

【问题 3】

- (4) 52:54:AB:34:5B:09
- (5) 192.168.1.100
- (6) 255.255.255.0
- (7) 192.168.1.254
- (8) 192.168.1.3

试题四分析

问题 1 解析

由题意可知，DHCP 服务器分别为网络 1 和网络 2 提供 IP 地址分配，其中网络 A 可分配的 IP 地址排除 DHCP 服务器占用的 110.115.3.3、FTP 服务器占用的 110.115.3.2，以及路由器 R1 一端端口占用的 110.115.3.1，剩余可分配的 IP 地址为 110.115.3.4~110.115.3.254。网络 2 中根据路由器 R1 的端口地址算出其 IP 范围为：61.202.117.193~61.202.117.254，再排除掉 WEB 服务器和路由器占用的地址，范围为 61.202.117.193~61.202.117.252。

问题 2 解析

DHCP 服务器提供动态 IP 地址分配，客户机通过广播和单播的方式获得 IP 地址，如果客户机是 Windows 系列操作系统，你会看到一个动态过程——正在获取 IP 地址……若是网内没有 DHCP 服务器或者服务器出现故障，那么 Windows 操作系统会从微软私有 IP 地址范围内 169.254.0.1~169.254.255.254 去获得一个 IP 地址。

问题 3 解析

Hosts 文件是一个用于存储计算机网络中节点信息的文件，它可以将主机名映射到相应的 IP 地址，实现 DNS 的功能，它可以由计算机的用户进行控制。Hosts 文件的存储位置在不同的操作系统中并不相同，在 Windows 操作系统下的目录通常为 c:\windows\system32\drivers\etc\。为了提高对经常访问的网络域名的解析效率，可以通过利用 Hosts 文件中建立域名和 IP 的映射关系来达到目的。根据 Windows 系统规定，在进行 DNS 请求以前，Windows 系统会先检查自己的 Hosts 文件中是否有这个网络域名映射关系。如果有则调用这个 IP 地址映射，如果没有，再向已知的 DNS 服务器提出域名解析。也就是说 Hosts 的请求级别比 DNS 高。

问题 4 解析

本题考查 FTP 服务器的配置，其中 IP 地址为 110.115.3.2。

问题 5 解析

根据图 13-4 和图 13-5，可以看出 110.115.3.10 主机可以访问虚拟目录，访问 FTP 虚拟目录的命令为：ftp://110.115.3.2:2121/pcn。

试题四参考答案

【问题 1】

- (1) 110.115.3.4~110.115.3.254 (2) 61.202.117.193~61.202.117.252

【问题 2】

不能正常访问 Internet。当 DHCP 服务器出故障时，APIPA 在 169.254.0.1 到 169.254.255.254 的私有空间内分配地址，所有设备使用默认的网络掩码 255.255.0.0。APIPA

存在于所有流行的各种版本的 Windows 系统中。

【问题 3】

(3) Hosts (4) 61.202.117.253

【问题 4】

(5) 110.115.3.2

【问题 5】

110.115.3.10, (6) ftp://110.115.3.2:2121/pcn

试题五分析

问题 1 解析

所谓静态路由配置，也就是用户人为地指定对某一网络访问时所要经过的路径。其中最关键的配置语句是：

```
Router> ip route ip-addr subnet-mask gateway
```

ip-addr 为 IP 地址，subnet-mask 为子网掩码，gateway 为网关。其中 IP 地址指的是目标网络的地址，而网关处的 IP 地址则说明了路由的下一站。

默认路由是一种特殊的静态路由，指的是当路由表中与包的目的地址之间没有匹配的表项时路由器能够做出的选择，如果没有默认路由器，那么目的地址在路由表中没有匹配表项的包将被丢弃。默认路由会大大简化路由器的配置，减轻管理员的工作负担，提高网络性能。

问题 2 解析

访问控制列表用来限制使用者或设备，达到控制网络流量，解决拥塞，提高安全性等目的。在 IP 网络中，可以使用的访问列表有标准访问列表（值为 1~99）、扩展访问列表（标号为 100~199）两种。

其中标准访问列表具体介绍如下。

基于源 IP 地址来进行判定是否允许数据报通过（或其他操作，例如在 NAT 中就是判断是否进行地址转换）。

命令格式：

```
access-list access-list-number {permit | deny}  
{source [ source-wildcard] | any }
```

命令解释如下。

access-list：访问列表命令。

access-list-number：访问列表号码，值为 1~99。

permit：允许。

deny：拒绝。

source：源 IP 地址。

source-wildcard：源 IP 地址的通配符。

any：任何地址，代表 0.0.0.0 255.255.255.255。

通配符：source-wildcard 省略时，则使用默认值 0.0.0.0。它的作用与子网掩码是不相同的，当其取值为 1 时，代表该位不必强制匹配；当其取值为 0 时，代表必须匹配。

因此，如果 source 是 203.66.47.0，source-wildcard 是 0.0.0.255，则说明只要前三组符合，最后一组可以不符合，即有一个 C 类的 IP 地址符合。

这个命令的实例如下：

```
access-list 1 permit 202. 1. 2.3 （允许 IP 地址为 202.1.2.3 的数据报通过）
```

```
access-list 2 permit 202. 1. 2.3 0.0.0.255 （允许网络 202.1.2.0 的数据报通过）
```

`access-list 3 deny 202. 1. 2.3` （禁止 IP 地址为 202.1.2.3 的数据报通过）

`access-list 5 deny 202. 1. 2.3` （禁止 IP 地址为 202.1.2.3 的数据报通过，但允许其他任何 IP 的数据报通过）

`access-list 5 permit any`

策略路由是一种比基于目标网络进行路由更加灵活的数据报路由转发机制。应用了策略路由，路由器将通过路由图决定如何对需要路由的数据报进行处理，路由图决定了一个数据报的下一跳转发路由器，配置过程如下：

- ① 使用 `route-map` 命令创建 `route map`；
- ② 使用 `match` 命令定义检查条件；
- ③ 使用 `set` 配置命令定义如果条件匹配后的行为。

问题 3 解析

`ip nat inside`: 指定与内部网络相连的内部端口。

`ip nat outside`: 指定与外部网络相连的外部端口。

试题五参考答案

【问题 1】

- (1) 0.0.0.0.0.0.0.10.10.10.1
- (2) 255.254.0.0
- (3) 10.10.20.1
- (4) 255.255.240.0
- (5) 10.10.20.1

【问题 2】

- (6) 10.10.30.2
- (7) 0.1.255.255
- (8) 0.0.15.255
- (9) `match`
- (10) `set`
- (11) 10.10.20.1

【问题 3】

- (12) 10.10.10.1
- (13) 255.255.255.0
- (14) 55.23.12.98
- (15) 255.255.255.252

全国计算机技术与软件专业技术 资格（水平）考试用书

网络工程师考试考前冲刺与考点分析

内容超值，针对性强

本书紧扣考试大纲，基于每个章节知识点分布统计分析的结果，科学地编写强化练习题，结构科学、重点突出、针对性强。

作者权威，阵容强大

希赛教育（www.educity.cn）专业从事人才培养、教育产品开发、教育图书出版，在职业教育方面具有极高的权威性。特别是在在线教育方面，稳居国内首位，希赛教育的远程教育模式得到了国家教育部门的认可和推广。

在线测试，心中有数

上学吧（www.shangxueba.com）在线测试平台为考生准备了在线测试，其中有数十套全真模拟试题和考前密卷，考生可选择任何一套进行测试。测试完毕，系统自动判卷，立即给出分数。

互动讨论，专家答疑

希赛教育软考学院是中国最大的软考在线教育网站，该网站论坛是国内人气最旺的软考社区，在这里，读者可以和数十万考生进行在线交流，讨论有关学习和考试的问题。希赛教育软考学院拥有强大的师资队伍，为读者提供全程的答疑服务，在线回答读者的提问。



责任编辑：孙学瑛
封面设计：李玲

上架建议：计算机考试

ISBN 978-7-121-20499-9



9 787121 204999 >

定价：59.00元